Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	GN Docket 20-109;
	)	ITC-214-20010613-00346;
	)	ITC-214-20020716-00371;
China Telecom (Americas) Corporation	)	ITC-T/C-20070725-00285

RESPONSE OF CHINA TELECOM (AMERICAS) CORPORATION TO ORDER TO SHOW CAUSE

REDACTED – FOR PUBLIC INSPECTION

Andrew D. Lipman
Catherine Wang
Russell M. Blau
Raechel Keay Kummer

MORGAN, LEWIS & BOCKIUS LLP
1111 Pennsylvania Ave., NW
Washington, D.C. 20004
(202) 739-3000
(202) 739-3001 (Fax)
andrew.lipman@morganlewis.com
catherine.wang@morganlewis.com
russell.blau@morganlewis.com
raechel.kummer@morganlewis.com

Counsel to China Telecom (Americas) Corporation

June 8, 2020

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	GN Docket 20-109;
	)	ITC-214-20010613-00346;
	)	ITC-214-20020716-00371;
China Telecom (Americas) Corporation	)	ITC-T/C-20070725-00285

RESPONSE OF CHINA TELECOM (AMERICAS) CORPORATION TO ORDER TO SHOW CAUSE

China Telecom (Americas) Corporation ("CTA"), by its undersigned counsel, hereby responds to the Order to Show Cause[1] ("Order") by the Federal Communications Commission ("FCC" or "Commission") in the above-captioned dockets.

The Order directs CTA "to explain why the Commission should not institute a proceeding" to revoke and terminate its domestic and international section 214 authorizations, and should not reclaim its International Signaling Point Codes ("ISPCs"). It further directs CTA to "file a written response providing evidence that it is not subject to the exploitation, influence, and control of the Chinese government, and of its ongoing qualifications to hold domestic and international section 214 authorizations and to hold ISPCs, thereby demonstrating that the public convenience and necessity would be served by its retention of the authorizations and assignments."[2]

---

[1] *See China Telecom (Americas) Corporation*, Order to Show Cause, DA-448, GN Docket 20-109, ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285 (rel. April 24, 2020) ("Order"). The Commission granted CTA an extension of time to respond to the Order to June 8, 2020. Letter from Denise Coca, Chief, Telecommunications and Analysis Division, International Bureau, Federal Communications Commission, to Andrew D. Lipman, Counsel for China Telecom (Americas) Corporation, DA 20-515, GN Docket 20-109, ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285 (May 14, 2020) ("May 14, 2020 Extension and Clarification Order").

[2] Order, ¶ 11.

As a matter of law, however, CTA does not have the burden to demonstrate that it is qualified to retain its authorizations. The Commission's inquiry unfairly and improperly places the burden on CTA to prove a negative regarding unspecified national security concerns about "exploitation" and "influence" of the Chinese government. These vague terms are left undefined in the Order or, to CTA's knowledge, anywhere in the FCC's rules or decisions. The Order leaves CTA to guess what these terms might mean or encompass.

Rather, as discussed in more detail in Exhibit 16, the Communications Act and Commission precedent permit revocation of CTA's authorizations only if there is clear and convincing evidence of egregious misconduct by CTA. Neither the Order nor the Recommendation of the Executive Branch agencies[3] provides even a *prima facie* basis for the Commission to make such a finding. CTA responds fully to the questions posed in the Order, but without waiving its objections to the legal insufficiency of the grounds cited therein.

CTA is responding to the Recommendation as an independent, profit-seeking business based in the United States, operating in the United States, serving many U.S. customers, and employing many U.S. citizens and permanent residents among its employees.

The bulk of CTA's response is contained in its answers to the questions posed in paragraph 12 of the Order, since those questions (particularly questions 14, 15 and 16) encompass all the issues the Commission has directed CTA to address. As shown in those answers, CTA is a Delaware corporation that is subject to U.S. law, and is not "subject to the exploitation, influence, and control of the Chinese government." CTA funds its business operation through revenues generated

[3] Executive Branch Recommendation to the Federal Communications Commission to Revoke and Terminate China Telecom Americas' International Section 214 Common Carrier Authorizations, File Nos. ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285, at 1 (filed Apr. 9, 2020) ("Recommendation").

from customers in arm's length commercial transactions. CTA is not subsidized by any foreign government and operates as an autonomous, profit-seeking enterprise. CTA's management is responsible to its parent company for fulfilment of commercial objectives. That parent company itself a publicly-traded corporation that is subject to statutory obligations to its shareholders and to disclosure requirements under both Hong Kong and U.S. securities laws. CTA's operations serve the public convenience and necessity by providing efficient, competitive, and high-quality bandwidth connections for businesses needing to exchange data between the United States and China; and resold mobile phone service for consumers and businesses needing dual telephone numbers and/or access to Chinese-speaking support and service staff.

Further, the Executive Branch Recommendation does not present sufficient grounds for the Commission to consider revoking CTA's authorizations. The Recommendation does not even acknowledge the controlling legal standard for revocation. Most of its factual allegations involve potential or imagined future conduct by third parties, not actual misconduct by CTA (much less "egregious" misconduct). There are only two sets of allegations in the Recommendation that relate specifically to CTA's own conduct, and these are addressed fully in Exhibit 16. First, the Recommendation takes issue with CTA's communication with Team Telecom concerning storage of CTA's customer records and its cybersecurity policies, but both of these claims are based on misinterpretations of CTA's statements. Second, the Recommendation alleges that CTA violated its Letter of Assurance ("LOA") with Team Telecom in two respects. But neither claim is correct. The claim regarding cybersecurity measures essentially argues that CTA violated a requirement that does not actually appear in its LOA, to provide a single, written set of cybersecurity policies.

And the claim regarding CTA's requests for assignments of ISPCs relies on an unreasonable, hypertechnical interpretation of the LOA (which, even if the Commission were to accept it, would not rise to the level of "egregious" misconduct).

Finally, even if the Commission were to credit the purely hypothetical risks suggested by the Recommendation, none of which have actually occurred, the Commission would have to consider whether there is a remedy short of revocation that would foreclose these risks while preserving the services used by thousands of CTA customers. Team Telecom's summary refusal even to consider potential mitigation measures is not justified.

CTA provides the following responses to the Commission's specific questions in paragraph 12 of the Order.

(1) A detailed description of the current ownership and control (direct and indirect) of the company and the place of organization of each entity in the ownership structure

RESPONSE: Please see Exhibit 1.

(2) A description of the ownership and control of the company when it was assigned international section 214 authorization, ITC-214-20010613-00346, effective June 7, 2002 and when it was granted international section 214 authorization, ITC-214-20020716-00371, on August 21, 2002

RESPONSE: Please see Exhibit 2.

(3) A detailed description of its corporate governance

RESPONSE: Please see Exhibit 3.

(4) An identification of China Telecom Americas' officers, directors, and senior management officials, their employment history (including prior employment with the Chinese government), and their affiliations with the Chinese Communist Party and the Chinese government

RESPONSE: Please see Exhibit 4.

(5) An identification of all CTL and China Telecom officers, directors, and other senior management, their employment history (including prior employment with the Chinese government), and their affiliations with the Chinese Communist Party and the Chinese government

RESPONSE: Please see Exhibit 5.

(6) A description of the services that China Telecom Americas provides in the United States and the specific services provided using the domestic and international section 214 authorizations as well as services it provides in the United States that do not require section 214 authority

RESPONSE: Please see Exhibit 6.

(7) An identification of the equipment used to provide telecommunications service, including the manufacturer, and the location of the equipment

RESPONSE: Please see Exhibit 7.

(8) A description and listing of China Telecom Americas' subscribers and other customers for domestic and international services[4]

RESPONSE: Please see Exhibit 8.

(9) A detailed description regarding the nature of the use of China Telecom Americas' ISPCs, including sufficient detail to understand the network scope, geographic coverage, and the public switched telephone network (PSTN) portions of the network; and the region(s) where China Telecom Americas uses the ISPCs in its PSTN network

RESPONSE: Please see Exhibit 9.

(10) A statement regarding the physical addresses where China Telecom Americas' ISPCs are located

RESPONSE: Please see Exhibit 10.

(11) A network diagram that shows how China Telecom Americas' ISPCs are used

RESPONSE: Please see Exhibit 11.

(12) A list of all physical points of interconnection between China Telecom Americas and other carriers as well as the names of each carrier with which China Telecom Americas interconnects

RESPONSE: Please see Exhibit 12.

(13) A list and copies of all interconnection agreements that China Telecom Americas has with other carriers

[4] The Commission clarified and narrowed the scope of this Request in the May 14, 2020 Extension and Clarification Order.

RESPONSE: Please see Exhibit 13.

(14) An explanation as to why the Commission should not reclaim China Telecom Americas' ISPCs

RESPONSE: Please see Exhibit 14.

(15) A description of the extent to which China Telecom Americas is or is not otherwise subject to the exploitation, influence, and control of the Chinese government

RESPONSE: Please see Exhibit 15.

(16) A detailed response to the allegations raised in the Executive Branch Recommendation to Revoke, requesting that the Commission revoke and terminate China Telecom Americas' international section 214 authorizations

RESPONSE: Please see Exhibit 16.

CTA respectfully submits there are no legally sufficient grounds, and no cause in fact, for the Commission to initiate a proceeding to revoke its authorizations. Nonetheless, if the Commission does "initiate a proceeding" for revocation, such proceeding must be an adjudicatory hearing before an Administrative Law Judge. In every previous case in which the Commission has considered revocation of a Section 214 authorization, except for inactive carriers that failed to respond to notices from the Commission, the carrier has been afforded an opportunity for an evidentiary hearing.[5]

[5] *See, e.g., In re Kurtis J. Kintel*, 22 FCC Rcd 17197 (2007) (order to show cause requiring an evidentiary hearing; proceeding was later terminated pursuant to a settlement agreement); *In re NOS Comm'cns, Inc.*, 18 FCC Rcd 6952, 6954, FCC 041-01 (2003) (order to show cause requiring an evidentiary hearing; proceeding was later terminated pursuant to a consent order); *In re Business Options, Inc.*, 18 FCC Rcd 6881, 6881-82, FCC 03-68 (2003) (order to show cause requiring an evidentiary hearing; proceeding was later terminated pursuant to a consent order); *In re Publix Network Corp.*, 17 FCC Rcd 11487, 11503, FCC 02-173 (2002) (order to show cause requiring an evidentiary hearing; proceeding was later terminated pursuant to consent decree); *In re CCN, Inc., et al.*, 12 FCC Rcd 8547, 8548, FCC 98-76 (1997) (order to show cause requiring an evidentiary hearing; hearing was terminated because licensees failed to file a written appearance). The Commission has also issued preliminary Orders to Show Cause, such as the one in this case, in several other proceedings that did not result in either an evidentiary hearing or a final order.

In the event of a hearing, CTA reserves the right to present additional evidence regarding the matters addressed in this response. At such a hearing, the Commission will have the burden of proof,[6] and CTA must have the ability respond to any evidence or argument that the Commission may present against it. CTA cannot reasonably be expected to anticipate at this time all allegations and arguments that may arise during a future proceeding.

[6] *See* Exhibit 16, Section II; and 47 C.F.R. § 1.91(d) (providing that "[i]n all such revocation and/or cease and desist hearings, the burden of proceeding with the introduction of evidence and the burden of proof shall be upon the Commission").

Respectfully submitted,

/s/ Andrew D. Lipman

Andrew D. Lipman
Catherine Wang
Russell M. Blau
Raechel Keay Kummer

MORGAN, LEWIS & BOCKIUS LLP
1111 Pennsylvania Ave., NW
Washington, D.C. 20004
(202) 739-3000
(202) 739-3001 (Fax)
andrew.lipman@morganlewis.com
catherine.wang@morganlewis.com
russell.blau@morganlewis.com
raechel.kummer@morganlewis.com

Counsel to China Telecom (Americas) Corporation

June 8, 2020

EXHIBIT 1

"A detailed description of the current ownership and control (direct and indirect) of the company and the place of organization of each entity in the ownership structure."

China Telecom (Americas) Corporation ("CTA"), a Delaware corporation, is a wholly owned direct subsidiary of China Telecom Corporation Limited ("CTCL") a company whose shares are publicly traded on the New York Stock Exchange (NYSE: CHA) and the Stock Exchange of Hong Kong Limited. CTCL was incorporated under the laws of the People's Republic of China. CTCL is a subsidiary of China Telecommunications Corporation ("CT"), which is also organized under the laws of the People's Republic of China. As of April 30, 2020,[1] CT owns approximately 70.89% of the outstanding shares of CTCL. Of the remaining shares, 11.96% are held by several entities registered or organized under the laws of the People's Republic of China: Guangdong Rising Assets Management Co. Ltd. (6.94%); Zhejiang Financial Development Company (2.64%); Fujian Investment & Development Group co., Ltd. (1.2%); and Jiangsu Guoxin Group Limited (1.18%). The remaining 17.15% of CTCL shares are widely held by shareholders trading on the public exchange, including Citigroup Inc., BlackRock, Inc., GIC Private Limited, the Bank of New York Mellon Corporation, JPMorgan Chase & Co., and Franklin Resources, Inc. CT is a corporation incorporated in Beijing, China, with its capital invested by the State-owned Assets Supervision and Administration Commission of the State Council ("SASAC") of the People's Republic of China.

[1] *See* CTCL, Form 13-G (Apr. 30, 2020), https://www.sec.gov/Archives/edgar/data/38777/000003877720000107/chin20a14.htm; CTCL, Annual Report (Form 20-F) (Apr. 23, 2020), https://www.sec.gov/Archives/edgar/data/1191255/000119312520123302/d851335d20f.htm#rom851335_9 ("CTCL 2019 20-F Report").

Please see Exhibit 1-1, attached, for an illustration of the current ownership and control of CTA and the place of organization of each entity in the ownership structure.

While CTA is a wholly owned subsidiary of CTCL and is indirectly owned by CT, CTA operates its U.S. business as an independent profit-making commercial enterprise. More detail regarding the relationship between CTA and its parent company is set forth in the answers to Requests #3 and #15.

EXHIBIT 1-1

China Telecom (Americas) Corporation Structure

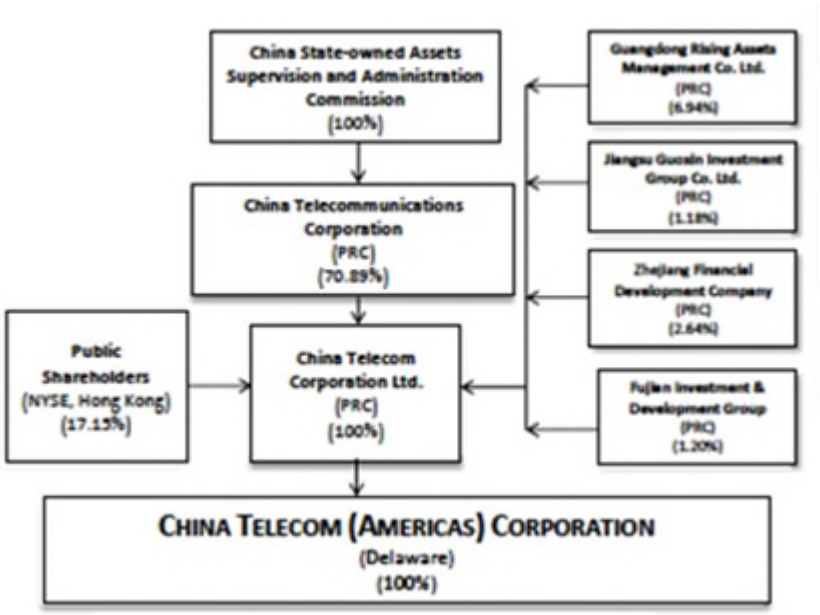


EXHIBIT 2

"A description of the ownership and control of the company when it was assigned international section 214 authorization, ITC-214-20010613-00346, effective June 7, 2002 and when it was granted international section 214 authorization, ITC-214-20020716-00371, on August 21, 2002."

At the time China Telecom (Americas) Corporation ("CTA") received its initial Section 214 authorizations from the FCC on June 7, 2002, and August 21, 2002 (File Nos. ITC-214-20010613-00346 and ITC-214-20020716-00371, respectively), it was operating as China Telecom (USA) Corp. ("CTUSA"), a Delaware corporation, and was a wholly owned, direct subsidiary of China Telecommunications Corporation ("CT"), a state-owned enterprise of the People's Republic of China.[1]

[1] We note that ITC-214-20010613-00346 was initially issued to CT on July 20, 2001, and assigned to CTUSA through a *pro forma* transaction consummated on June 7, 2002. On July 12, 2007, CT transferred all of the stock in CTA to China Telecom Corporation Limited ("CTCL"), a company organized under the law of the People's Republic of China with majority ownership by CT. *See* ITC-T/C-20070725-00285, Public Notice, International Authorizations Granted, Report No. TEL-01179, DA No. 07-3632 (Rel. Aug. 16, 2007).

EXHIBIT 3

"A detailed description of its corporate governance."

A. Introduction

China Telecom (Americas) Corporation's ("CTA" or the "Company") is a profit-making, commercial enterprise that operates on a day-to-day basis independently and without interference from its parent company on core business matters including investment, vendor relations, sales, service provisioning, billing and accounting, collection and receivables, financing, labor, contracts, legal affairs, regulatory compliance and other business matters. CTA is governed in accordance with its Bylaws as well as its Certificate of Incorporation. As discussed below, review and approval by China Telecom Corporation Limited ("CTCL") is required for certain major corporate or business changes but CTA's day-to-day operations and decision-making are independent of its parent company and managed by its executive officers with oversight from its Board of Directors ("Board").

B. Oversight

As is customary in corporate governance under U.S. law,[1] CTCL, as CTA's direct parent and sole shareholder, reviews and approves certain major decisions. Consistent with functions and rights regarding various important corporate matters granted to the stockholders in CTA's Bylaws, as the sole stockholder, CTA's immediate corporate parent, CTCL oversees and approves certain major decisions, including decisions on significant expenditures, projects, investments, and other commercial obligations.

[1] *See, e.g.*, *infra* n.2, regarding Delaware Law provisions and case law with respect to controlling shareholders' voting power over certain major decisions.

Consistent with Delaware corporate law recognizing the rights of majority stockholders,[2] CTA's Bylaws authorize CTCL, as the sole stockholder of CTA, to examine the Board's reports, approve the increase or reduction of CTA's authorized shares of capital stock, approve merger, division, dissolution or liquidation of CTA to the extent required under the Delaware General Corporate Law, approve and amend CTA's core institutional documents, and approve other major matters which are subject to the approval of stockholders. CTCL may also authorize or delegate to the Board to carry out such matters.

C. Board of Directors

Pursuant to the Company's Bylaws, the Board may have no less than five (5) members, with the number to be determined from time to time by resolution of the Board. As the sole stockholder in CTA, CTCL has the power to elect, remove and replace directors. Directors are elected annually, and may not conduct any business, or hold any other office or place of profit in any other company that creates a conflict of interest with CTA or otherwise conflicts with CTA's internal policies. Each Director is elected for a term of one year, after which the Director may stand for re-election and reappointment for subsequent terms.

The Board has authority to determine CTA's long term strategic plans, annual business plans and business operation plans. Certain specific matters are subject to Board approval: CTA's annual financial budget and final accounts; issuance of debt and other financing activities; opening,

---

[2] Delaware corporate law provides for shareholder influence over major business decisions either through communications with board members and management or through formal voting *Paramount Commc'ns Inc. v. QVC Network Inc.*, 637 A.2d 34, 42 (Del. 1994) (recognizing controlling stockholder's voting power to "(a) elect directors; (b) cause a break-up of the corporation; (c) merge it with another company; (d) cash-out the public stockholders; (e) amend the certificate of incorporation; (f) sell all or substantially all of the corporate assets; or (g) otherwise alter materially the nature of the corporation and the public stockholders' interests."); *see* DEL. CODE ANN. tit. 8, §§ 211, 242, 251–258, 263, 271, 275.

cancellation or other change to CTA's bank accounts; procurement of material assets in a single transaction; the engagement of accounting firms; the disposition, transfer, or acquisition of large-amount assets of CTA; changes to CTA's organizational structure and fundamental policies and rules; issuance of debentures and grants of guarantees or securities; donations to and sponsorship of third parties; CTA's investment plans, including changes to representative offices or subsidiaries and other equity investment matters such as write-off losses of equity investments; and to establish or amend fundamental policies and documents of CTA, including with respect to decision-making policies consistent with Delaware corporate law for the exercise by the Board of Directors and Officers of their respective duties.

The Board appoints one of its directors to act as Chairman of the Board. In this capacity, the Chairman sets the agenda for and presides over Board meetings, organizes the implementation of Board duties and status of resolutions, signs securities certificates issued by CTA, and exercise duties assigned by the Board or the Bylaws.

D. Executive Officers

Under CTA's Bylaws, each officer shall be appointed or removed by a majority vote of the Board. The President is a member of the Board. The executive officers are President, Vice President, Secretary, and Treasurer. The powers and duties in the management of CTA are prescribed by the Board, and generally are as follows:

- **President**: The President is the chief executive officer of the corporation, responsible for managing the daily business of CTA and delegating responsibilities to other officers, senior managers and other employees as appropriate to implement the budget approved by the Board, the annual business operation plan, marketing and promotion plan. The President makes decisions necessary to implement specific tasks such as signs contracts,

leases, bonds, and other legal instruments and other important documents on behalf of CTA; deals with disputes, accidents, and emergencies; and approves basic operation rules.

- **Vice-President**: The Vice-President assumes all the duties of the President in his or her absence, and performs other duties as the President designates.

- **Secretary**: The Secretary attends all sessions of the Board and acts as clerk thereof, and records all the votes of CTA and the minutes.

- **Treasurer**: The Treasurer keeps full and accurate accounts of receipts and disbursements in books belonging to CTA. The Treasurer keeps the moneys of CTA in a separate account to the credit of CTA and disburses the funds of CTA.

E. CTA OPERATIONS

CTA's day-to-day operations are independent of its parent company. While CTA is a wholly owned subsidiary of CTCL and is indirectly owned by China Telecommunications Corporation ("CT"), CTA operates its U.S. business as an independent profit-making commercial enterprise with respect to capital investment, vendor relations, sales, provision of service, billing and accounting, collection and receivables, financing, labor, contractors, regulatory compliance and other business matters. In practice, CTA management develops and manages its own annual investment plan and puts forward its budget requirements for approval by the CTA Board. In the beginning of each fiscal year, CTA negotiates its annual budget with CTCL. Once this budget is set, CTA has broad discretion over its daily business and operations within the scope of the budget.

CTA manages its own payroll, employee recruitment, commissions, labor costs and planning, negotiates contracts with its customers, acceptable pricing margins, procures its facilities,

vendor management and service providers, including accounting and law firms. CTA negotiates with CTCL and CT on an arms-length basis regarding the terms and conditions for purchases and utilization of their products and services, including pricing, as it does with non-affiliated customers.

In connection with marketing services that include CT products and services to U.S. customers, CTA maintains its own provisioning, engineering and pricing teams to customize solutions for individual customers. CTA also maintains its own service agreement templates and conducts its own pricing and provisioning negotiations with customers. Similarly, for CTA's mobile service offerings, CTA determines the specific offerings, marketing, promotion, and operational details to comply with U.S. federal and state requirements.

CTA manages the procurement of network elements and services and operates its own Network Operations Center ("NOC") in **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]** for CTA customer resources in the Americas region. CTA manages its own provisioning and acceptance processes and deals directly with customers on service issues, including under applicable service level agreements. CTA manages its fixed and intangible assets, including inventory, leasing, transfer, and adjustments.

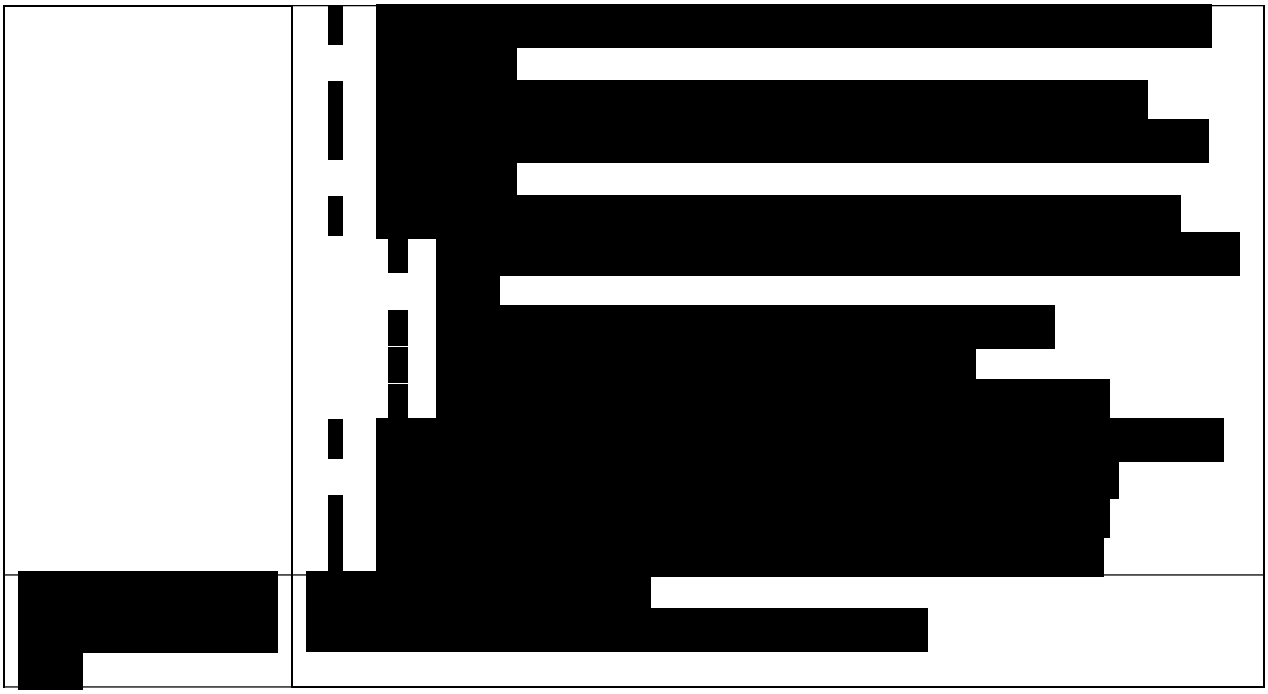
CTA manages its own customer and supplier contracts as well as legal compliance in accordance with applicable U.S. law and corporate best practices, including establishment of internal corporate policies and compliance with federal and state regulatory and other legal requirements. CTA maintains its own legal staff and outside legal resources.

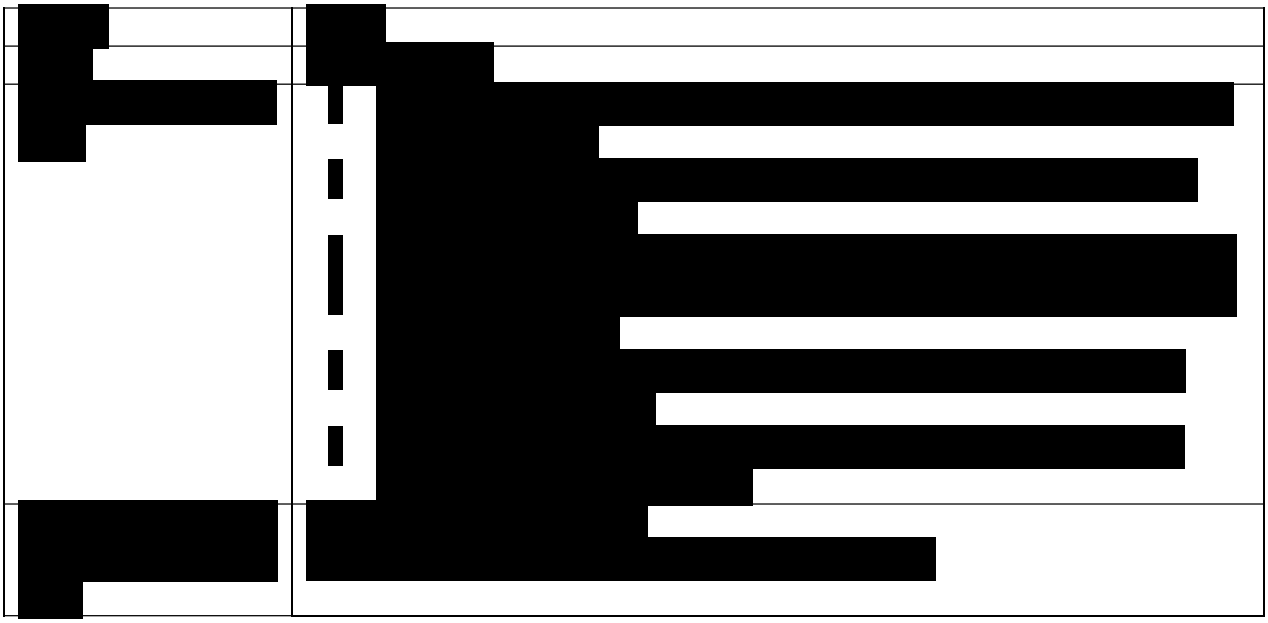
EXHIBIT 4

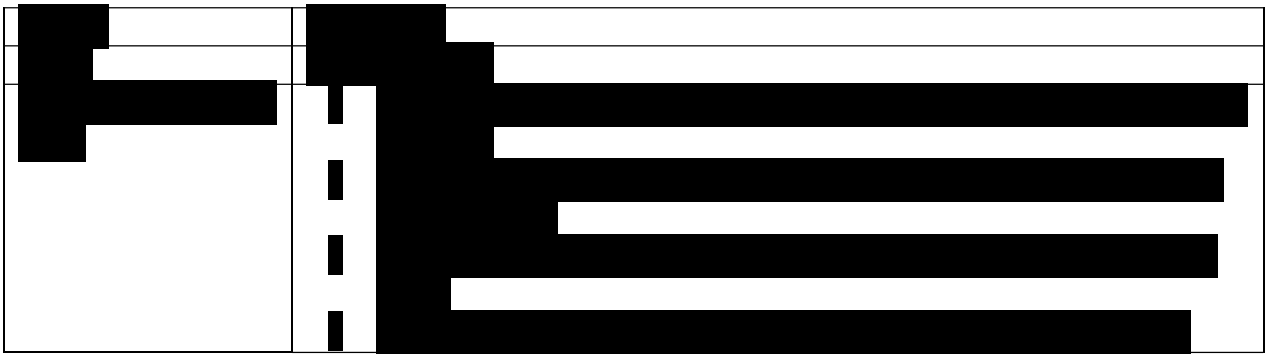
"An identification of China Telecom Americas' officers, directors, and senior management officials, their employment history (including prior employment with the Chinese government), and their affiliations with the Chinese Communist Party and the Chinese government."

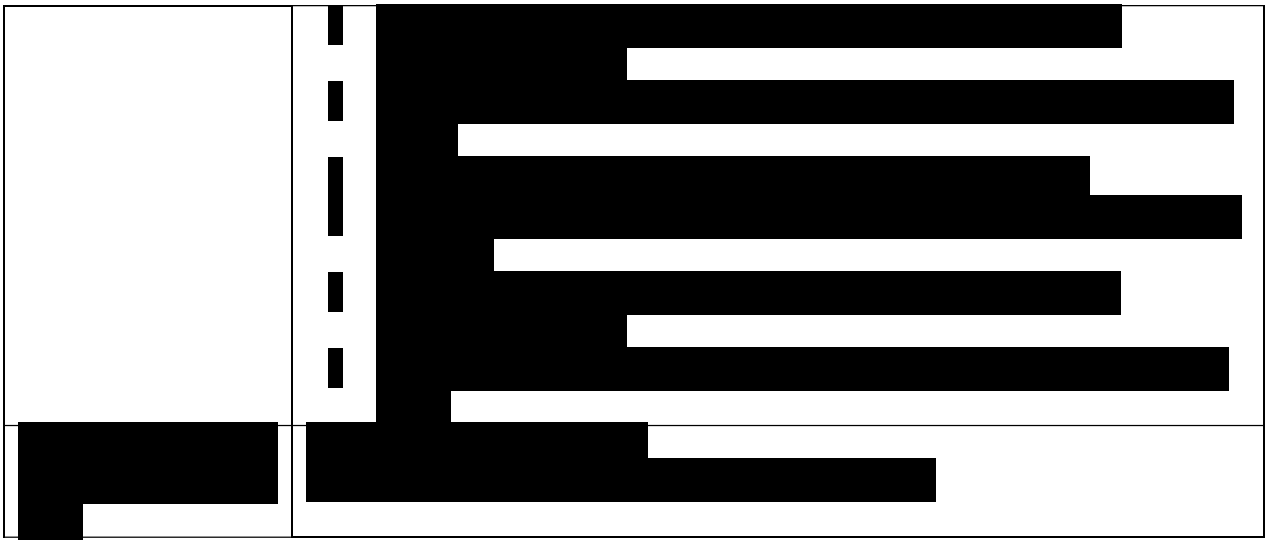
The current officers and directors of China Telecom (Americas) Corporation are as follows: **[BEGIN CONFIDENTIAL]**

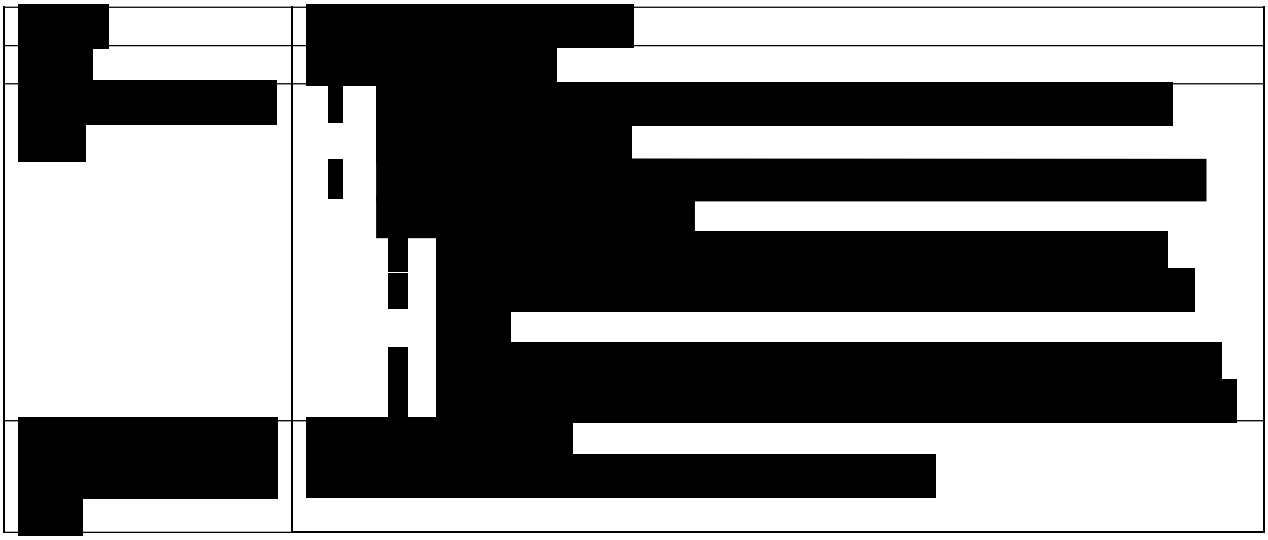
[redacted]

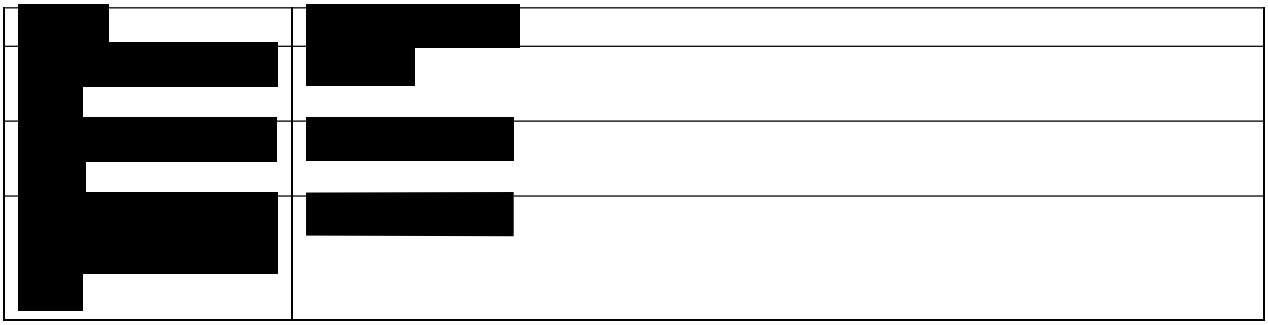


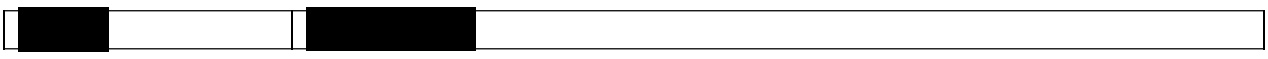


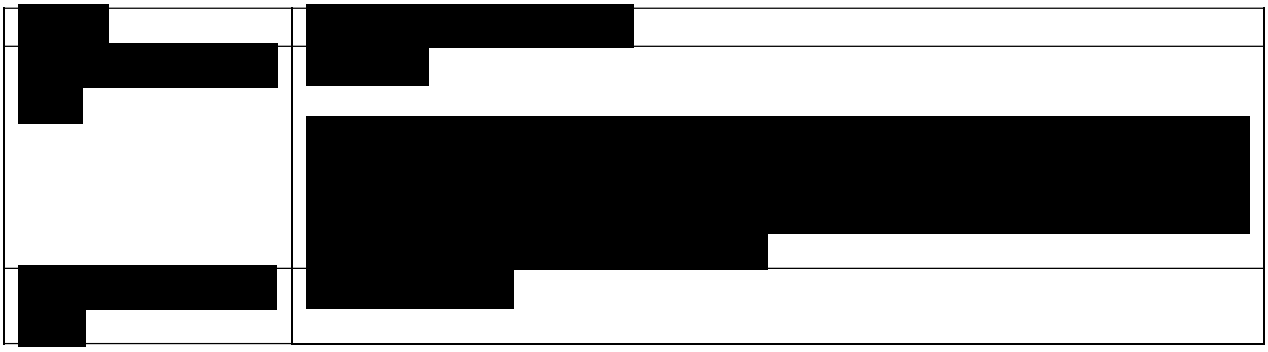












[redacted]

[END CONFIDENTIAL]

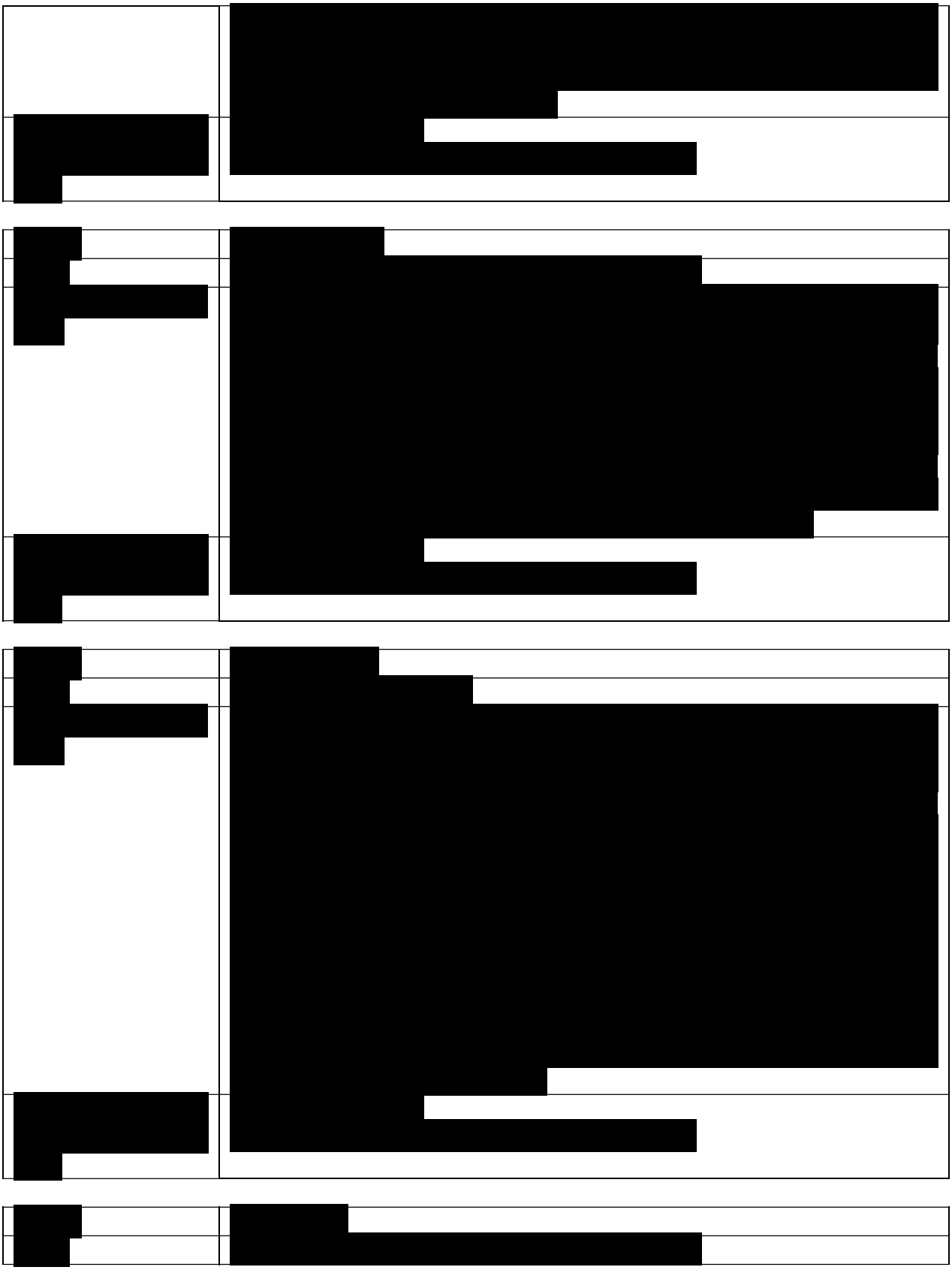
EXHIBIT 5

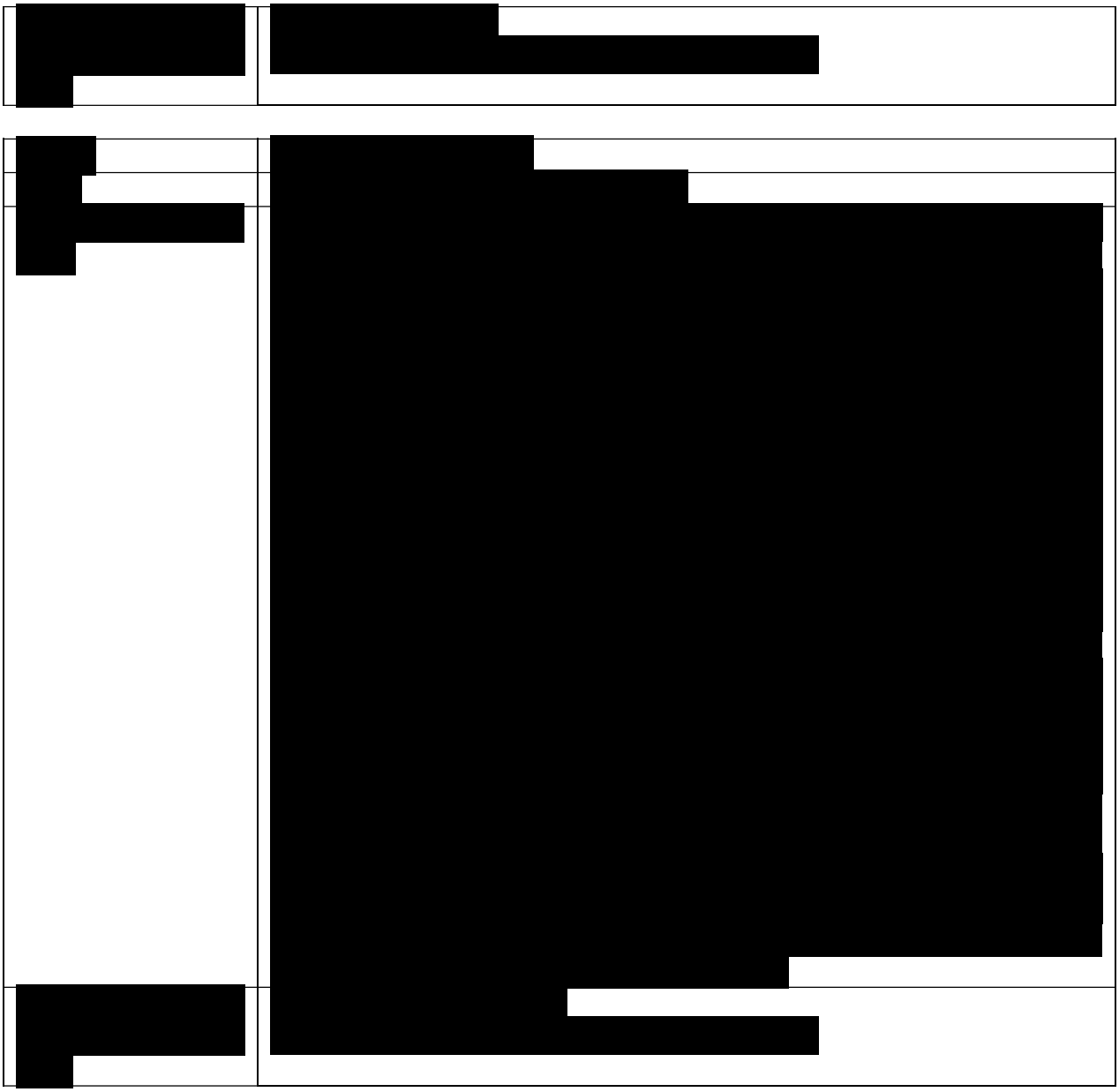
"An identification of all CTL and China Telecom officers, directors, and other senior management, their employment history (including prior employment with the Chinese government), and their affiliations with the Chinese Communist Party and the Chinese government."

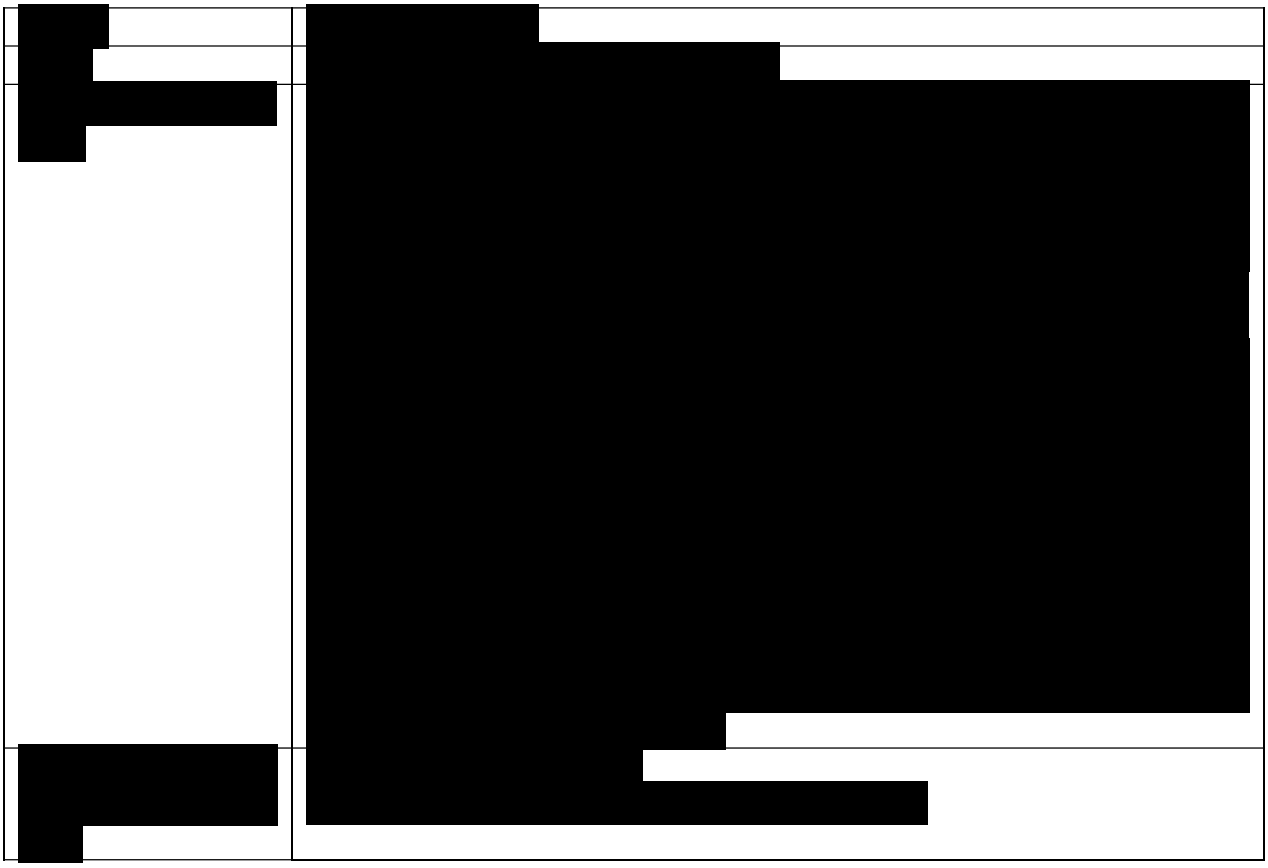
[BEGIN CONFIDENTIAL]

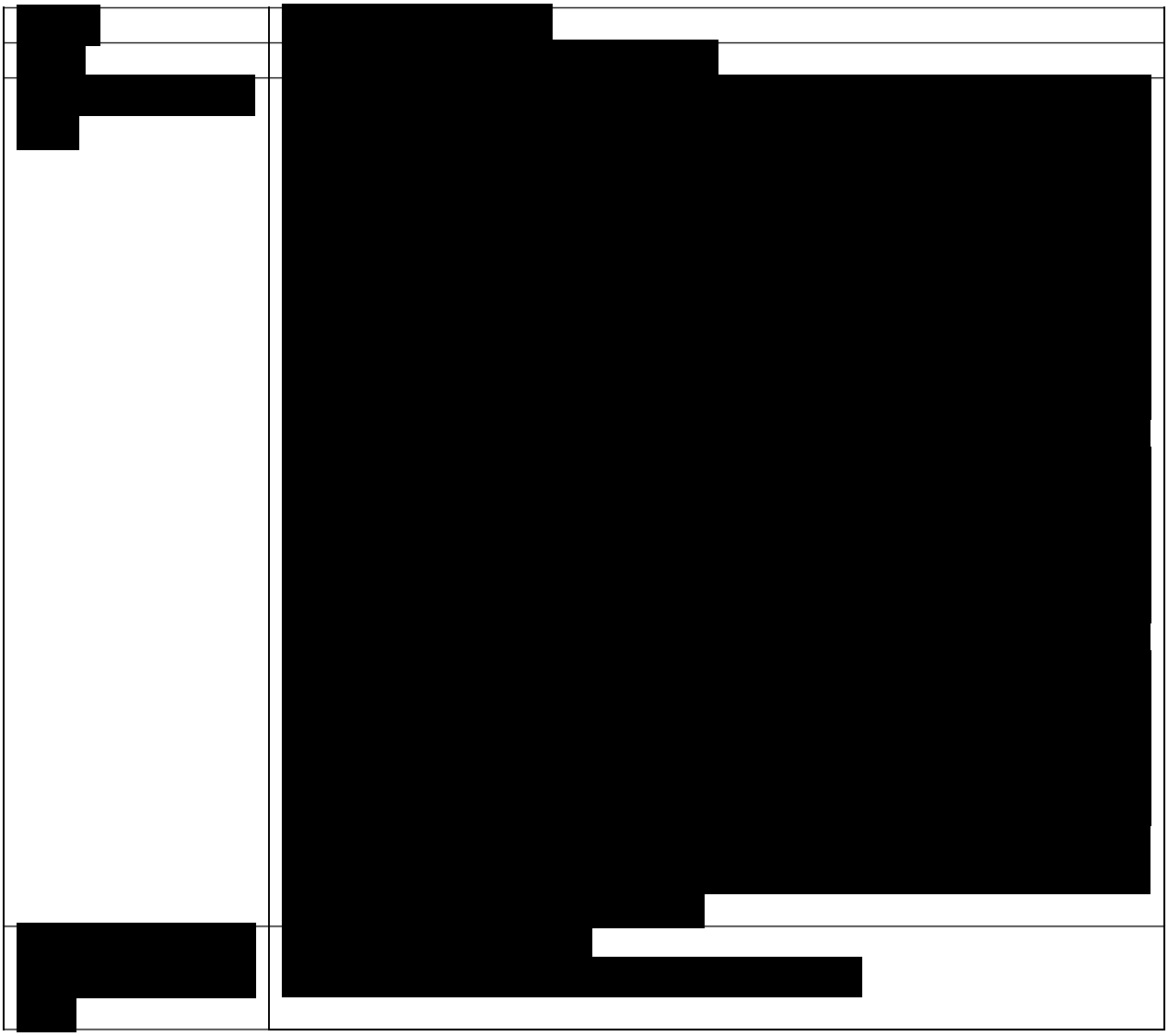
I. [redacted]

[redacted]

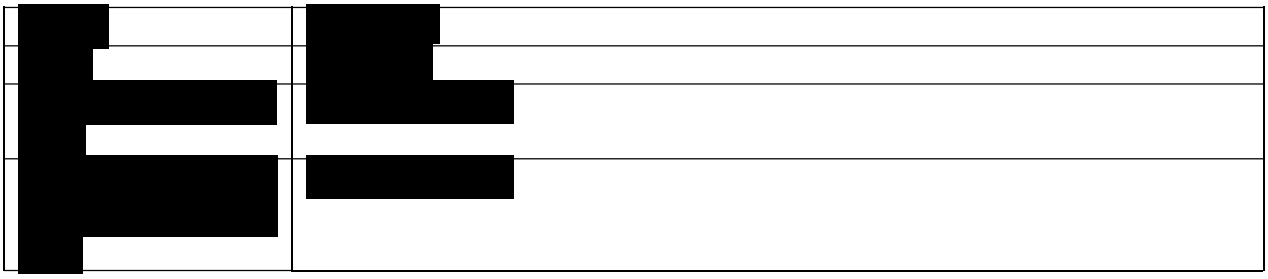








II.



[END CONFIDENTIAL]

EXHIBIT 6

"A description of the services that China Telecom Americas provides in the United States and the specific services provided using the domestic and international section 214 authorizations as well as services it provides in the United States that do not require section 214 authority."

China Telecom (Americas) Corporation ("CTA") provides a variety of services in the U.S., including both telecommunications and non-telecommunications services. Some telecommunications capabilities are provided as common carrier services pursuant to domestic and/or international section 214 authorizations, while some are provided on a private carrier basis. Although CTA holds indefeasible rights of use ("IRUs"), CTA leases but has not constructed underlying long haul and local distribution lines in the United States. CTA provides communications and Internet-based services to its customers by leasing lines from other carriers and providing the switching, routing and related equipment and value-added services necessary to meet customer request for services as detailed below. CTA leases its lines from major U.S. facilities-based carriers and infrastructure providers such as **[BEGIN HIGHLY CONFIDENTIAL]** [redacted]. **[END HIGHLY CONFIDENTIAL]** CTA provides the communications services described below by providing leased private lines from a customer's designated location to a CTA POP or a customer may arrange for a third party carrier to deliver the customer's traffic to CTA's POP. From its POP, CTA provides leased lines to submarine cable landing stations for access to international submarine cables that terminate international traffic to China and other non-U.S. points. CTA is not a local exchange carrier and does not itself provide customers access to the PSTN.

CTA's customers in the United States are U.S. enterprises, telecommunications carriers, and Chinese enterprises in the United States. In addition, CTA provides resold mobile services to

consumers as a mobile virtual network operator ("MVNO") under the brand name "CTExcel," which is a common carrier service.

In addition to CTA's MVNO service, the Recommendation claims that CTA provides international private line and leased circuits,[1] MPLS VPN,[2] SD-WAN,[3] virtual private local area network ("LAN") services,[4] data center and cloud services,[5] and services such as Managed Security and Managed WAN as a managed service provider.[6] As explained further below, CTA provides only limited service offerings in the United States. CTA is an international telecommunications company helping connect U.S. enterprises to China and other Asian destinations, or Chinese enterprises to the United States. The Company depends on local partners in both the United States and China to fulfill customer solutions.

I. Communications and Internet Services

CTA's business primarily facilitates telecommunications services in China for American companies under U.S. contracts through resale of other carriers' facilities and services, including those of CTA's affiliates and non-affiliated service providers (including U.S. carriers). CTA's largest market segment is providing data services and Internet related services to enterprise and carrier customers. For most customers, CTA functions only as the connectivity provider focused primarily on delivering data communication services between the United States and China.

---

1 Recommendation, p. 8.

2 Recommendation, p. 9.

3 *Id.*

4 *Id.*

5 Recommendation, p. 10.

6 Recommendation, p. 11.

A. International Private Leased Circuits

CTA provides international private leased circuits ("IPLCs"). IPLC is a service operating on part of China Telecommunications Corporation's ("CT's") global transmission network providing cross-border or cross-regional customers with fully transparent end-to-end international private dedicated circuit services with fixed bandwidth guarantees for an exclusive end customer. IPLC uses Synchronous Digital Hierarchy ("SDH"), Synchronous Optical Network ("SONET"), or Optical Transport Network ("OTN") technology.

IPLC does not traverse the public Internet. An IPLC can be used for Internet access, data transmission, video conferencing, and any other form of telecommunications.

B. International Ethernet Private Lines

CTA offers International Ethernet Private Line service ("IEPL"), a point-to-point or point-to-multipoint Ethernet services that provide flexible bandwidth and Ethernet access capabilities over a part of CT's transmission network, or with the interconnected partners' Ethernet network. The bandwidth options ranges from 2 Mpbs to 10 Gbps.

C. Global Wavelength

CTA's Global Wavelength service provides fully transparent circuit transmission services using CT's (including CTA's) and its partners' worldwide OTN or Wavelength Division Multiplexing ("WDM") transport networks. The typical bandwidths that can be provided are 10 Gbps and 100 Gbps.

D. Ethernet over MPLS

Ethernet over MPLS ("EoMPLS") is engineered to provide private communication over MPLS networks. It allows geographically dispersed sites to share an Ethernet broadcast domain by connecting sites through MPLS Tunnels and Virtual Circuits. Two services are offered using

this technology: Ethernet Virtual Private Line ("EVPL") or Virtual Leased Line ("VLL"), and Ethernet Virtual Private LAN ("EVPLAN" or "VPLS").

E. Multiple Protocol Label Switching/Virtual Private Network

CTA's MPLS-VPN service rides on CT's Multi-Protocol Label Switching ("MPLS") based bearer network called CN2 and interconnected carriers' MPLS networks. The service provides customers with highly secured data transmission for logical connectivity among multiple destinations. China Telecom CN2 is a business class IP network with high resiliency, supporting various business applications of priorities.

F. Internet Protocol Security VPN

CTA offers Internet Protocol Security ("IP Sec") VPN service, which allows a site to communicate with other MPLS VPN sites with Internet connectivity through IP Sec tunnels. IP Sec is a framework for a set of protocols for security at the network or packet processing layer of network communication. IP Sec VPN is an information service.

G. Internet Services

CTA's Global Internet Service is Internet access and transit services. To provide Global Internet Service, CTA uses both ChinaNet (AS 4134) and CN2 (AS 4809). CTA has its own peering and IP transit, but CTA's network is part of the global ChinaNet and CN2 network.

CTA markets and sells Internet Services on behalf of China Telecom Corporation Limited ("CTCL") and other affiliates. CTA also resells Internet services from other non-CT partners in the United States and other countries for enterprise customers. CTA's Internet services are information services.

H. MVNO Services

Since 2015, CTA has offered mobile services as a MVNO under the name "CTExcel." The CTExcel MVNO service is primarily targeted at consumers and a limited number of business customers.

CTA offers services as an MVNO through an MVNO aggregator called **[BEGIN HIGHLY CONFIDENTIAL]** [redacted] **[END HIGHLY CONFIDENTIAL]** the largest Mobile Virtual Network Enabler ("MVNE"), using the **[BEGIN HIGHLY CONFIDENTIAL]** [redacted] **[END HIGHLY CONFIDENTIAL]** mobile network. **[BEGIN HIGHLY CONFIDENTIAL]** [redacted] **[END HIGHLY CONFIDENTIAL]** maintains the direct commercial relationship with **[BEGIN HIGHLY CONFIDENTIAL]** [redacted] **[END HIGHLY CONFIDENTIAL]** and CTA buys services from **[BEGIN HIGHLY CONFIDENTIAL]** [redacted]. **[END HIGHLY CONFIDENTIAL]** Individual consumers purchase CTA's CTExcel SIM card and obtain service on a monthly basis for the plan of their choice.

All U.S. domestic calls are terminated within the **[BEGIN HIGHLY CONFIDENTIAL]** [redacted] **[END HIGHLY CONFIDENTIAL]** network. When an international call is established, **[BEGIN HIGHLY CONFIDENTIAL]** [redacted] **[END HIGHLY CONFIDENTIAL** routes the call to **[BEGIN HIGHLY CONFIDENTIAL]** [redacted] **[END HIGHLY CONFIDENTIAL]** a U.S. company. **[BEGIN HIGHLY CONFIDENTIAL]** [redacted] **[END HIGHLY CONFIDENTIAL]** sends the call to China Telecom Global Limited ("CTG") in Hong Kong. CTG then routes the international call from Hong Kong to a terminating carrier based on the destination of the dialed number.

CTExcel offers dual U.S. and Chinese telephone numbers on their phone as a service feature, allowing the user to have calls forwarded between their U.S. and China cell phone numbers.

I. SIP Trunking

CTA has a limited offering to businesses of SIP trunking service, an Internet-based method of sending voice and other messaging applications using IP-enabled PBX's. SIP trunking uses Session Initiation Protocol (SIP), the standard communications protocol for a Unified Communications (UC) solution across a data network.

II. Other Non-Communications Services

A. Internet Data Center Services

CTA procures space in the United States from some of the largest data center providers to resell space to its customers. Data center services offered by CTA include collocation space (including racks and cages), power, and cross connects (*i.e.*, in-house wiring within the data centers) to connect a data center customer to either a network provider or between data center customers in the same building. For most data center locations, a third-party provider is responsible for ongoing operation of the data center. CTA's Internet Data Center Service is not a telecommunications service.

B. Cloud Service

CTA resells cloud service, a service designed to provide customers the ability to utilize virtual computing resources to support customers' computing needs. Cloud Service is not a telecommunications service.

C. Virtual Private Cloud

CTA resells Virtual Private Cloud, which provides end users with a virtual data center which supports on-demand resources on request, elastic scaling, self-service and other functions. Virtual Private Cloud is not a telecommunications service.

D. Cloud Exchange

CTA's Cloud Exchange is a cloud access service that enables private connections to public cloud providers such as **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]**

E. SD-WAN

CTA resells SD-WAN, which is software-defined wide-area network service to deploy a management network with Software Defined Network ("SDN") technology and resources. SDN is an approach to network management that enables dynamic, programmatically efficient network configuration in order to improve network performance and monitoring making it more like cloud computing than traditional network management. SD-WAN is not a telecommunications service.

F. Customer Premises Equipment

CTA provides customer premises equipment ("CPE") such as routers and/or switches for purchase or lease by customers. Provision of CPE through purchase or lease to customers and is not a telecommunications service.

G. Equipment Leasing

CTA leases servers and/or other equipment to customers to allow the customer to connect to CTA's network. The leasing of equipment is not a telecommunications service.

H. Project Item

CTA's Project Item service represents a one-time service for project delivery and integration of various computing and communication technologies and hardware. Project Item is not a telecommunications service.

I. NetCare

CTA offers NetCare, which is an optional managed service that utilizes expert personnel, rigorous process and CT's unified customer network monitoring platform to deliver real-time, pro-active connectivity monitoring and network troubleshooting to clients. NetCare is not a telecommunications service.

J. Maintenance Service

CTA's Maintenance Service represents a full range of onsite network and IT maintenance service following the initial installation and integration of customer equipment. CTA's Maintenance Service is not a telecommunications service.

K. Anti-DDoS Service

CTA's Anti-DDoS service detects real-time Distributed Denial of Service ("DDoS") attacks through the connected network and activates the protection procedures set by customer. **[BEGIN HIGHLY CONFIDENTIAL]** [redacted] **[END HIGHLY CONFIDENTIAL]** is the mitigation solution usually adopted to reroute attacking traffic, scrubbing and re-injecting clean traffic back to customer's network. This is not a telecommunications service.

L. Global Media Distribution and Exchange

CTA provides Global Media Distribution & Exchange ("MDX"), a product leveraging CTA's affiliates' state-of-the-art territory-wide network in China, together with overseas on-net and off-net transmission resources, into a media one-stop-solution for the current global professional broadcasting community. **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]**

M. Information and Communications Technologies

CTA offers professional Information and Communications Technologies ("ICT") service through local partners. ICT is a comprehensive solution through the integration of communications and information products.

EXHIBIT 7

"An identification of the equipment used to provide telecommunications service, including the manufacturer, and the location of the equipment."

Below is a list of China Telecom (Americas) Corporation ("CTA") equipment, including manufacturer and locations, that CTA currently uses as of April 24, 2020. The list is ordered alphabetically by state and city. CTA interprets the Commission's request as seeking information regarding CTA's network transmission equipment currently used in the United States in providing CTA's telecommunications services to end users. This equipment is listed below. In addition, in the interest of providing a thorough response, CTA also identifies certain network equipment used for transmission services that may not be classified as "telecommunications services" (*e.g.*,

[BEGIN HIGHLY CONFIDENTIAL] [redacted]

[redacted]**. [END HIGHLY CONFIDENTIAL]**

[BEGIN CONFIDENTIAL]
1. [redacted]

[END CONFIDENTIAL]

Category	Manufacturer	Model Type	Usage
[BEGIN HIGHLY CONFIDENTIAL]			
[redacted]			

[END HIGHLY CONFIDENTIAL]

[BEGIN CONFIDENTIAL]
2. [redacted]
[END CONFIDENTIAL]

Category	Manufacturer	Model Type	Usage
[BEGIN HIGHLY CONFIDENTIAL]			
[redacted]			
[END HIGHLY CONFIDENTIAL]			

[BEGIN CONFIDENTIAL]
3. [redacted]
[END CONFIDENTIAL]

Category	Manufacturer	Model Type	Usage
[BEGIN HIGHLY CONFIDENTIAL]			
[redacted]			
[END HIGHLY CONFIDENTIAL]			

[BEGIN CONFIDENTIAL]
4. [redacted]
[END CONFIDENTIAL]

Category	Manufacturer	Model Type	Usage
[BEGIN HIGHLY CONFIDENTIAL]			
[redacted]			
[END HIGHLY CONFIDENTIAL]			

[BEGIN CONFIDENTIAL]
5. [redacted]
[END CONFIDENTIAL]

Category	Manufacturer	Model Type	Usage
[BEGIN HIGHLY CONFIDENTIAL]			
[redacted]			
[END HIGHLY CONFIDENTIAL]			

[BEGIN CONFIDENTIAL]
6. [redacted]
[END CONFIDENTIAL]

Category	Manufacturer	Model Type	Usage

[BEGIN HIGHLY CONFIDENTIAL]			
[redacted]	[redacted]	[redacted]	[redacted]

[END HIGHLY CONFIDENTIAL]

[BEGIN CONFIDENTIAL]

7. [redacted]

[END CONFIDENTIAL]

Category	Manufacturer	Model Type	Usage
[BEGIN HIGHLY CONFIDENTIAL]			
[redacted]	[redacted]	[redacted]	[redacted]

[END HIGHLY CONFIDENTIAL]

[BEGIN CONFIDENTIAL]

8. [redacted]

[END CONFIDENTIAL]

Category	Manufacturer	Model Type	Usage
[BEGIN HIGHLY CONFIDENTIAL]			
[redacted]	[redacted]	[redacted]	[redacted]

[END HIGHLY CONFIDENTIAL]

[BEGIN CONFIDENTIAL]

9. [redacted]

[END CONFIDENTIAL]

Category	Manufacturer	Model Type	Usage
[BEGIN HIGHLY CONFIDENTIAL]			
[redacted]	[redacted]	[redacted]	[redacted]

[END HIGHLY CONFIDENTIAL]

[BEGIN CONFIDENTIAL]

10. [redacted]

[redacted]
[END CONFIDENTIAL]

Category	Manufacturer	Model Type	Usage
[BEGIN HIGHLY CONFIDENTIAL]			
[redacted]			

[END HIGHLY CONFIDENTIAL]

[BEGIN CONFIDENTIAL]
11. [redacted]
[END CONFIDENTIAL]

Category	Manufacturer	Model Type	Usage
[BEGIN HIGHLY CONFIDENTIAL]			
[redacted]			

[END HIGHLY CONFIDENTIAL]

[BEGIN CONFIDENTIAL]
12. [redacted]
[END CONFIDENTIAL]

Category	Manufacturer	Model Type	Usage
[BEGIN HIGHLY CONFIDENTIAL]			
[redacted]			

[END HIGHLY CONFIDENTIAL]

[BEGIN CONFIDENTIAL]
13. [redacted]
[END CONFIDENTIAL]

Category	Manufacturer	Model Type	Usage
[BEGIN HIGHLY CONFIDENTIAL]			

[redacted]

[END HIGHLY CONFIDENTIAL]

[BEGIN CONFIDENTIAL]

14. [redacted]

[END CONFIDENTIAL]

Category	Manufacturer	Model Type	Usage
[BEGIN HIGHLY CONFIDENTIAL]			
[redacted]			

[END HIGHLY CONFIDENTIAL]

[BEGIN CONFIDENTIAL]

15. [redacted]

[END CONFIDENTIAL]

Category	Manufacturer	Model Type	Usage
[BEGIN HIGHLY CONFIDENTIAL]			
[redacted]			

[END HIGHLY CONFIDENTIAL]

[BEGIN CONFIDENTIAL]

16. [redacted]

[END CONFIDENTIAL]

Category	Manufacturer	Model Type	Usage
[BEGIN HIGHLY CONFIDENTIAL]			
[redacted]			

[redacted]

[END HIGHLY CONFIDENTIAL]

[BEGIN CONFIDENTIAL]

17. [redacted]

[END CONFIDENTIAL]

Category	Manufacturer	Model Type	Usage
[BEGIN HIGHLY CONFIDENTIAL]			
[redacted]			

[END HIGHLY CONFIDENTIAL]

[BEGIN CONFIDENTIAL]

18. [redacted]

[END CONFIDENTIAL]

Category	Manufacturer	Model Type	Usage
[BEGIN HIGHLY CONFIDENTIAL]			
[redacted]			

[END HIGHLY CONFIDENTIAL]

[BEGIN CONFIDENTIAL]

19. [redacted]

[END CONFIDENTIAL]

Category	Manufacturer	Model Type	Usage
[BEGIN HIGHLY CONFIDENTIAL]			
T[redacted]			

[END HIGHLY CONFIDENTIAL]

[BEGIN CONFIDENTIAL]

20. [redacted]

[END CONFIDENTIAL]

Category		Manufacturer	Model Type	Usage
[BEGIN HIGHLY CONFIDENTIAL]				
[redacted]		[redacted]	[redacted]	

[END HIGHLY CONFIDENTIAL]

[BEGIN CONFIDENTIAL]

21. [redacted]

[END CONFIDENTIAL]

Category	Manufacturer	Model Type	Usage
[BEGIN HIGHLY CONFIDENTIAL]			
[redacted]	[redacted]	[redacted]	[redacted]

[END HIGHLY CONFIDENTIAL]

[BEGIN CONFIDENTIAL]

22. [redacted]

[END CONFIDENTIAL]

Category	Manufacturer	Model Type	Usage
[BEGIN HIGHLY CONFIDENTIAL]			
[redacted]	[redacted]	[redacted]	[redacted]

[END HIGHLY CONFIDENTIAL]

[BEGIN CONFIDENTIAL]

23. [redacted]

[END CONFIDENTIAL]

Category	Manufacturer	Model Type	Usage
[BEGIN HIGHLY CONFIDENTIAL]			
[redacted]	[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]		[redacted]
[END HIGHLY CONFIDENTIAL]			

EXHIBIT 8

"A description and listing of China Telecom Americas' subscribers and other customers for domestic and international services."

Request No. 8 seeks "a description and listing of China Telecom Americas' subscribers and other customers for domestic and international services." By letter dated May 14, 2020, the Commission responded to China Telecom (Americas) Corporation's ("CTA's") earlier inquiry regarding Request No. 8 and stated: "we hereby clarify and narrow the scope of Request No. 8 as set forth below: . . ." The Commission therein provided additional detail of its request with respect to CTA's enterprise, MVNO mobile resale, other customers, and Chinese government customers.

For the purpose of responding to Request No. 8, CTA herein provides information regarding its subscribers and other customers for CTA's communications services most of which are classified as telecommunications services. In the interest of providing a thorough response, CTA also includes customers and subscribers for CTA's communications services that may not be classified as telecommunications services (e.g., Internet services) as well as non-communications services (*e.g.*, IDC). CTA interprets the Commission's request with respect to domestic services as seeking customer information regarding CTA's communications services that originate and terminate within the United States, and the Commission's request with respect to international services as seeking customer information regarding CTA's communications services that originate and terminate between the United States and a non-U.S. point. For non-communications services, CTA provides customer information for services provided in the United States. Relevant timeframes for the information provide are specified below. Unless otherwise specified, CTA interprets the Commission's requests with respect to "contract type" as seeking the description of services provided by CTA.

I. Enterprise Customers

Enterprise Customers. With respect to China Telecom Americas' enterprise customers, we request the name and a short description of each enterprise customer; a general description of the types and duration (e.g., yearly, monthly, or other) of enterprise customer contracts; the aggregate number of customers for each type of contract; and the most recent annual revenue derived from enterprise customers.

CTA provides three broad categories of service to enterprise customers. First, CTA provides services that it categorizes as "Communications and Internet Services" ("C/I") which includes international private leased circuits ("IPLC"), international Ethernet private lines ("IEPL"), Global Wavelength, EoMPLS, MPLS-VPN, IP Sec, Internet Services, SIP Trunking, Netcare, and Anti-DDoS. Second, CTA provides Internet Data Center and Cloud Services ("IDC/C") which includes Cloud, Virtual Private Cloud, Cloud Exchange, and SD-WAN services. Third, CTA provides services it categorizes as Information and Communications Technologies ("ICT") which includes CPE, Project Item, equipment leasing, and other technology solution services. CTA offers contracts for any combination of these three categories. A list of the names of CTA's enterprise customers as of May 28, 2020, and short descriptions of each is provided in alphabetical order in Exhibit 8-1.[1] Table 8-1, below, lists the types of CTA's enterprise customer contracts and the aggregate number of customers by type of contract. For all types of contracts, CTA enters into contracts for one (1), three (3) or five (5) year terms.

Table 8-1. Aggregate Customers for Each Enterprise Contract Type

[BEGIN HIGHLY CONFIDENTIAL]

Contract Type	*Aggregate Number of Customers*
All services (C/I, ICT, and IDC/C)	[redacted]
C/I and ICT	[redacted]
C/I and IDC/C	[redacted]
ICT and IDC/C	[redacted]
ICT only	[redacted]

[1] Descriptions are provided based on publicly available information.

IDC/C only	[redacted]
C/I only	[redacted]

[END HIGHLY CONFIDENTIAL]

In FY 2019, CTA's annual revenue derived from CTA's enterprise customers for domestic and international services, as defined above, was approximately **[BEGIN HIGHLY CONFIDENTIAL]** [redacted] **[END HIGHLY CONFIDENTIAL]** USD.

II. MVNO Mobile Resale Service Customers

MVNO Mobile Resale Services Customers. With respect to China Telecom Americas' MVNO mobile resale services customers, we request the aggregate number of customers, rounded to the nearest one thousand as of April 24, 2020, broken down into categories of customers, such as enterprise and small business and/or consumer; a general description of the types and duration of customer contracts, plans, or services; the aggregate number of customers for each type of contract, plan, or service, rounded to the nearest one thousand as of April 24, 2020; and the most recent annual revenue derived from MVNO mobile resale services customers.

Table 8-2, below, provides aggregate numbers of customers for each type of MVNO customer as of April 24, 2020, broken down into categories of customers.

Table 8-2. Aggregate Customers for Each Customer Category

[BEGIN HIGHLY CONFIDENTIAL]

Category of Customer	*Aggregate Number of Customers*
Business	[redacted]
Individual	[redacted]

[END HIGHLY CONFIDENTIAL]

CTA provides three types of mobile resale services: prepaid, postpaid, and pay as you go. Table 8-3, below, outlines the aggregate number of customers for each type of contract as of April 24, 2020, broken down into categories of customers. CTA notes that for the purpose of aggregating the number of customers to respond to Request No. 8, business customers who purchased multiple

products will be counted multiple times in the aggregate count and, accordingly, the aggregated customer/category number does not indicate the absolute number of distinct customers.

Table 8-3. Aggregate Customers for Each MVNO Contract Type

[BEGIN HIGHLY CONFIDENTIAL]

Contract Type	*Duration*	*Aggregate Customers*
Business - Postpaid	Monthly	[redacted]
Individual - Prepaid	Monthly	
Individual – Pay As You Go	None	

[END HIGHLY CONFIDENTIAL]

In FY 2019, CTA's annual revenue derived from MVNO customers for domestic and international communications services, as defined above, was approximately **[BEGIN HIGHLY CONFIDENTIAL]** [redacted] **[END HIGHLY CONFIDENTIAL]** USD.

III. Other Customers

With respect to any other types of services offered by China Telecom Americas, we request a general description of the services and customers; the types and duration of customer contracts by service type; the aggregate number of customers for each type of contract as of April 24, 2020; and the most recent annual revenue derived from these customers.

In addition to the aforementioned enterprise customers and MVNO mobile resale services customers, CTA's also provides communications services, as defined above, on a wholesale basis to certain CTA affiliates. The types of communications services provided to the customers in this category are: (a) Communications and Internet Services ("C/I") including domestic and international IEPL, IPLC, and VPN; (b) cloud services; (c) IDC services; and (d) ICT services. CTA provides these services to its affiliates upon request and on an order-by-order basis to meet the specific requirements of the affiliates' customers. The duration of these orders vary but typically

are for one (1) year terms. Table 8-4, below, outlines the aggregate number of customers for each type of contract as of April 24, 2020.

Table 8-4. Aggregate Customers for Each Contract Type

[BEGIN HIGHLY CONFIDENTIAL]

Contract Type	*Aggregate Number of Customers*
C/I Only	[redacted]
C/I, Cloud, IDC, and ICT	[redacted]
C/I, IDC, and ICT	[redacted]

[END HIGHLY CONFIDENTIAL]

In FY 2019, CTA's annual revenue derived from this category of customers as defined above, was approximately **[BEGIN HIGHLY CONFIDENTIAL]** [redacted] **[END HIGHLY CONFIDENTIAL]** USD.

IV. Chinese Government Customers

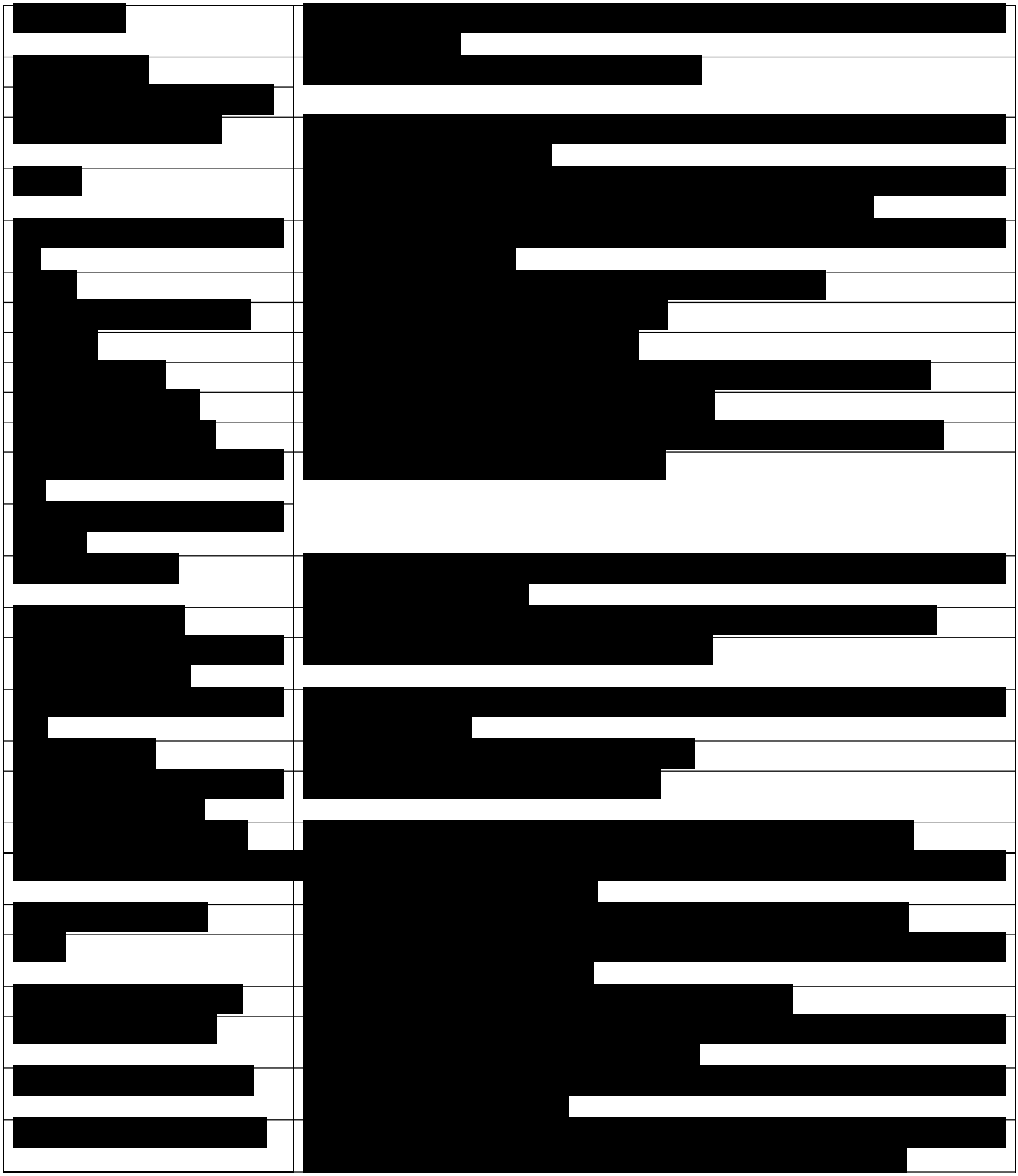
Chinese Government Customers. Please identify any customers that are affiliated with the government of the People's Republic of China or entities owned or controlled by, or otherwise connected to, the government and/or are members of the Communist Party of China.

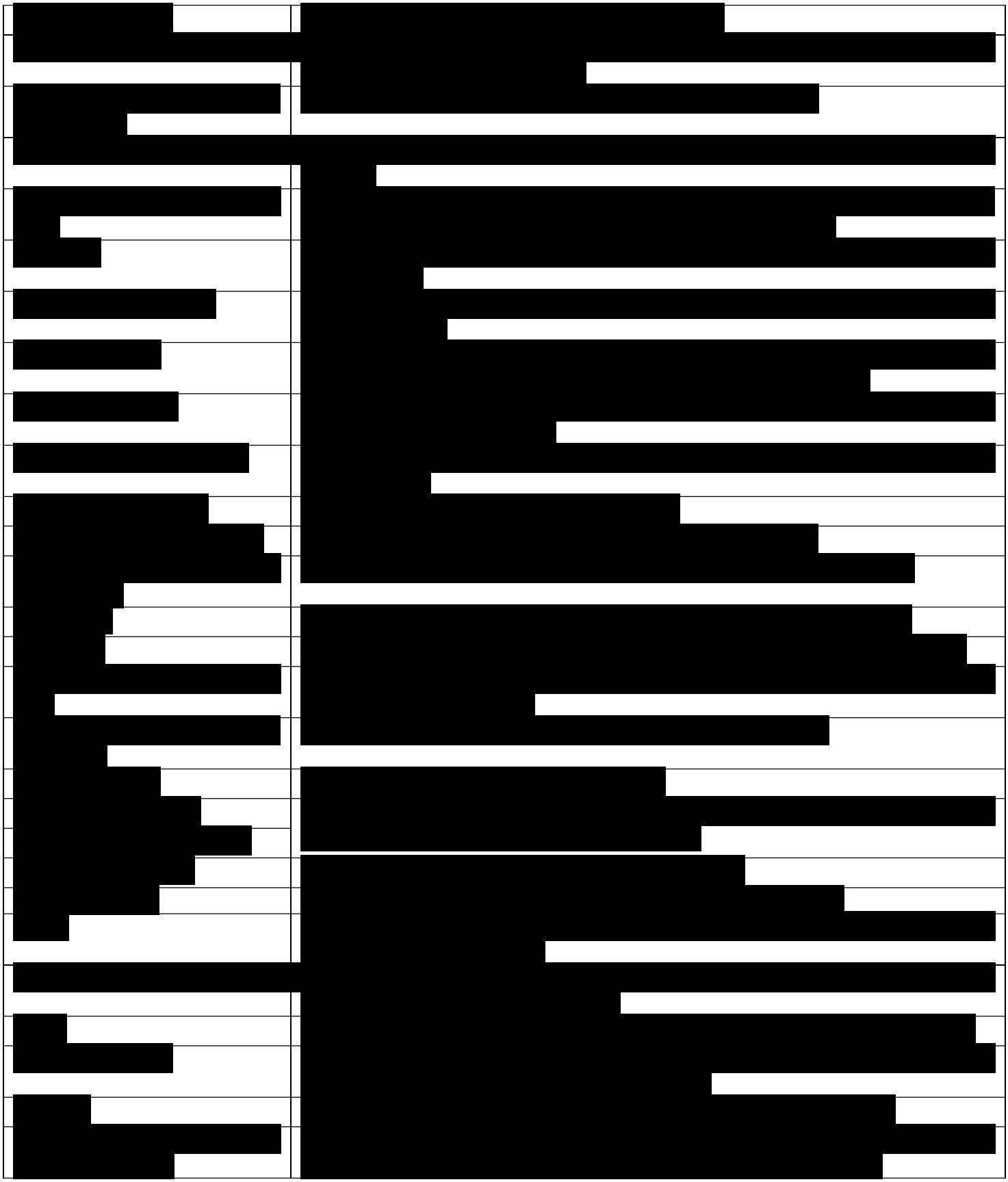
In its commercial purchasing and ordering process, CTA has not and does not collect information from its third-party customers as to ownership or control, or affiliation with any government, including the People's Republic of China, or any political party, including the Communist Party of China. Therefore, other than as identified below, CTA is not in a position to represent to the Commission the government ownership, control, or government or political affiliation of any of its third-party customers.

[BEGIN CONFIDENTIAL] [redacted] **[END CONFIDENTIAL] [BEGIN HIGHLY CONFIDENTIAL]** [redacted] **[END HIGHLY CONFIDENTIAL] [BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL] [BEGIN HIGHLY CONFIDENTIAL]** [redacted] **[END HIGHLY CONFIDENTIAL] [BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL] [BEGIN HIGHLY CONFIDENTIAL]** [redacted]**. [END HIGHLY CONFIDENTIAL]**

EXHIBIT 8-1
CTA ENTERPRISE CUSTOMERS
[BEGIN HIGHLY CONFIDENTIAL]

[redacted]	[redacted]
[redacted]	[redacted]





[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[END HIGHLY CONFIDENTIAL]	

EXHIBIT 9

"A detailed description regarding the nature of the use of China Telecom Americas' ISPCs, including sufficient detail to understand the network scope, geographic coverage, and the public switched telephone network (PSTN) portions of the network; and the region(s) where China Telecom Americas uses the ISPCs in its PSTN network."

China Telecom (Americas) Corporation ("CTA") has maintained three International Signaling Point Codes ("ISPCs"): one acquired in 2003 **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]** FCC File No. SPC-NEW-20030314-00014, granted on 3/17/2003) and two acquired in 2010 **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]** FCC File No. SPC-NEW-20100314-00006, granted on 03/17/2010; and **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]** FCC File No. SPC-NEW-20100326-00007, granted on 03/26/2010). CTA acquired these ISPCs in order to meet customer demand at that time for the provision of voice services. ISPCs are used where switching occurs or where switching signals are transmitted or received. ISPCs are needed in order for a Signaling System 7 ("SS7") to route calls properly. CTA completed its voice platform in 2003, launching a wholesale business to buy and sell large-scale voice capacity from international and U.S. carriers. CTA's use of the ISPCs was quite limited and involved only the use in two switches at CTA's Los Angeles, California location to support routing voice links to China. The ISPCs represented only one of the several technology approaches CTA used to provide routing for voice services.

CTA used the ISPC codes for its voice wholesale business which was a substantial part of CTA's business in the early stages of the company's growth. In response to the Commission's inquiry regarding CTA's public switched telephone network ("PSTN"), CTA clarifies that it did not maintain a PSTN for its wholesale voice service and does not maintain a PSTN today.

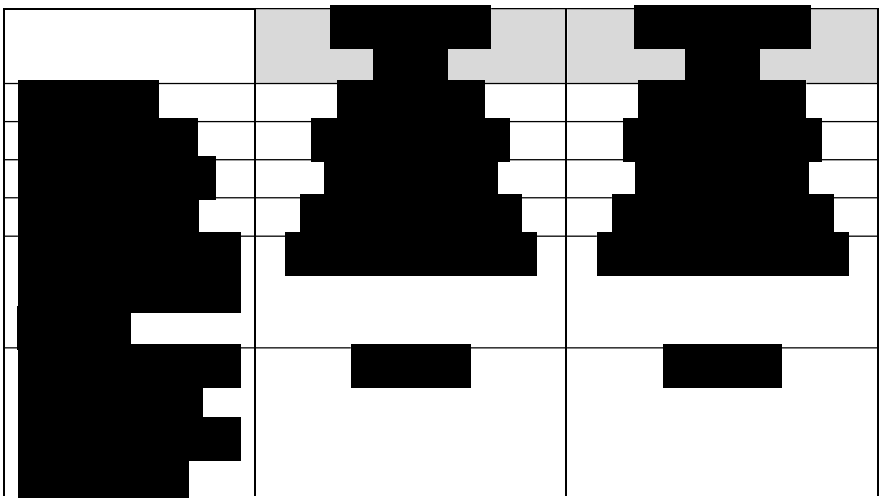
As fierce competition in the marketplace eroded CTA's business margin and increased bad debt accounts raised financial risk, CTA reduced and eventually ceased offering the wholesale

voice services between 2016 and 2018. The ISPCs were also used in CTA's MVNO service which CTA introduced in 2015. CTA ceased using the ISPCs for its MVNO service in February 2018. CTA used the ISPCs to facilitate services on its network until 2018 consistent with ITU procedures and seeks to retain the ISPCs for potential use in new services.

Table 9-1, below, provides an overview of CTA's ISPCs,[1] including their corresponding equipment; nature of use; network scope; geographic coverage; the PSTN portions of the network; the regions for which they were used; and the date on which each recent use of the ISPC was discontinued.

Table 9-1. CTA ISPC Use

[BEGIN CONFIDENTIAL]



[END CONFIDENTIAL]

[1] **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]** which was acquired shortly before [**BEGIN CONFIDENTIAL**] [redacted] **[END CONFIDENTIAL]** was not ultimately configured for use.

EXHIBIT 10

"A statement regarding the physical addresses where China Telecom Americas' ISPCs are located."

China Telecom (Americas) Corporation's ("CTA's") International Signaling Point Codes ("ISPCs") currently have no associated physical addresses. During the time that CTA utilized ISPCs to support its voice services, **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]** was configured on the voice switch located **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]** and **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]** was configured on the voice switch located at **[BEGIN CONFIDENTIAL]** [redacted]. **[END CONFIDENTIAL]**

EXHIBIT 11

"A network diagram that shows how China Telecom Americas' ISPCs are used."

[BEGIN CONFIDENTIAL] [redacted]

[redacted]

[END CONFIDENTIAL]

EXHIBIT 12

"A list of all physical points of interconnection between China Telecom Americas and other carriers as well as the names of each carrier with which China Telecom Americas interconnects."

At the outset, China Telecom (Americas) Corporation ("CTA") clarifies that it does not maintain interconnection agreements within the meaning of and subject to the requirements of Sections 251 and 271 of the Communications Act, as amended (the "Act").[1] CTA is not an incumbent local exchange carrier. CTA operates in a competitive, not monopoly, environment. Nonetheless, CTA's network does physically interconnect with other networks to provide customer service. Accordingly, for the purpose of responding to Request No. 12, CTA understands "carrier" to mean a company that provides telecommunications services to multiple end users, and "interconnection" as an agreement or arrangement with another carrier for the basic connection between networks in order to exchange traffic to provide customer services to multiple end users.[2] In the interest of providing a thorough response, CTA provides below a list of carriers with which CTA interconnects, as that term is defined above, as well as for the purpose of Internet peering. It is CTA's understanding that many of the companies listed below are "carriers" under the definition stated above but CTA has not confirmed the status of those companies and makes no representation regarding their status. **[BEGIN HIGHLY CONFIDENTIAL]**

[redacted]

[1] 47 U.S.C. §§ 251 and 271. Section 271 of the Act pertains to "interconnection" in accordance with Section 251 of the Act by which incumbent local exchange carriers are, among other things, subject to various requirements to interconnect with requesting carriers for the transmission and routing of telephone exchange service and exchange access.

[2] For these purposes, CTA has not included connections arranged for individual customers, *e.g.* local loops in an international private line leased circuit.

[redacted]

[redacted]

[3] [redacted].

[END HIGHLY CONFIDENTIAL]

A list of the physical points of interconnection between CTA and other carriers and companies noted above is provided alphabetically by state and city in Exhibit 12-1.

EXHIBIT 12-1
CTA PHYSICAL POINTS OF INTERCONNECTION
[BEGIN HIGHLY CONFIDENTIAL]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted] [redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted] [redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[END HIGHLY CONFIDENTIAL]

EXHIBIT 13

"A list and copies of all interconnection agreements that China Telecom Americas has with other carriers."

China Telecom (Americas) Corporation ("CTA") does not maintain interconnection agreements within the meaning of and subject to the requirements of Sections 251 and 271 of the Communications Act, of 1934, as amended (the "Act").[1] Accordingly, for the purpose of responding to Request No. 13, CTA understands "carrier" to mean a company that provides telecommunications services to multiple end users, and "interconnection" as an agreement or arrangement with another carrier for the basic connection between networks in order to exchange traffic to provide customer services to multiple end users. In response to Request No. 13, CTA provides a list and copies of its currently effective agreements for network interconnection, most of which are styled as "Master Service Agreements" that provide the general terms and conditions for interconnection arrangements between the parties. It is CTA's understanding that many of the companies listed below are "carriers" under the definition stated above but CTA has not confirmed the status of those companies and makes no representation regarding their status. In the interest of a thorough answer, CTA notes that it also interconnects with carriers and other companies for Internet peering (as listed in Exhibit 12), but typically does not enter into formal written agreements to do so. As noted below, CTA provides the one written agreement it has for a peering partner.

Please see Table 13-1, below, and attached exhibits, for copies of CTA's written agreements for interconnection, as defined above.

[1] 47 U.S.C. §§ 251 and 271. Section 271 of the Act pertains to "interconnection" in accordance with Section 251 of the Act by which incumbent local exchange carriers are, among other things, subject to various requirements to interconnect with requesting carriers for the transmission and routing of telephone exchange service and exchange access.

Table 13-1. List of Agreements

[BEGIN HIGHLY CONFIDENTIAL]

[redacted]

[2] [redacted]. **[END HIGHLY CONFIDENTIAL]**

EXHIBIT 14

"An explanation as to why the Commission should not reclaim China Telecom Americas' ISPCs."

China Telecom (Americas) Corporation ("CTA") currently holds three International Signaling Point Codes ("ISPC") assigned by the Commission.[1] The Order directs CTA to explain "why the Commission should not reclaim [CTA's] ISPCs[.]"[2] However, CTA is not aware of any reason why the Commission *should* reclaim these codes, and the Order did not propose any reason (other than, by implication, the same reasons offered for considering revoking CTA's Section 214 authorizations).

Reclaiming CTA's ISPCs would be inconsistent with the procedures governing ISPC assignments and withdrawals. Under the International Telecommunications Union ("ITU") ISPC Assignment Procedures, a national administration (*i.e.*, the Commission) is encouraged to withdraw an assignment if, for example, the ISPC is being used in a different way from that for which it was assigned, the resource is being used by an operator other than to whom the ISPC was assigned, or the assigned ISPC is no longer in use or required by the signaling point operator.[3] The ITU ISPC Assignment Procedures are not self-executing, however; they provide that national administrations "should publish their rules for use of, application for, and assignment of, ISPCs" including "a rationale for withdrawal of ISPCs[.]"[4] Therefore, the Commission's administration

---

[1] *See* SPC-NEW-20030314-00014; SPC-NEW-20100314-00006; SPC-NEW-20100326-00007.

[2] Order, ¶ 12.

[3] ITU, ITU-T Recommendation Q.708 (03/99), Art. 11.6, https://www.itu.int/rec/T-REC-Q.708-199903-I/en ("ITU ISPC Assignment Procedures").

[4] *Id.*

of ISPCs – including the assignment and reclamation of such codes – is supposed to be done pursuant to "publish[ed] … rules." However, the Commission has not adopted, and the Order does not cite, any rules governing ISPCs.[5] Consistent with ITU procedures, CTA used the ISPCs to facilitate services on its network and seeks to retain the ISPCs for potential use in new services. The Commission therefore should not reclaim CTA's ISPCs codes.

[5] The Order repeatedly cites to the ITU ISPC Assignment Procedures rather to any rules of the Commission.

EXHIBIT 15

A description of the extent to which China Telecom Americas is or is not subject to the exploitation, influence, and control of the Chinese government

Although China Telecom (Americas) Corporation ("CTA") is owned by a corporation that is incorporated in China, CTA is not subject or vulnerable to the "exploitation, influence, and control" of the Chinese government in the way alleged by the Executive Branch agencies in their Recommendation.[1] Rather, the Recommendation appears to confuse the government, state-owned enterprises ("SOEs") and their overseas subsidiaries, and to ignore the distinctions and independence of different entities under applicable law. The natural consequence of this view, however, is that the foreign corporation cannot enjoy the protection, stability and predictability of U.S. laws. Such a position may cause market participants to abandon or have to leave the U.S. market, or more accurately, to be deprived of the assets and businesses formed by their long-term diligent and compliant operations in United States.

As explained in Exhibit 1, CTA is a corporation organized and existing under the laws of the State of Delaware. CTA's direct parent is China Telecom Corporation Limited ("CTCL"), a public company listed on the Hong Kong Stock Exchange ("HKEx") and New York Stock Exchange ("NYSE"). As a publicly-traded company, CTCL has always been transparent about its ownership structure, including by making regular public filings with the Securities Exchange Commission ("SEC") and the HKEx. CTCL's controlling shareholder is China Telecommunications

[1] *See* Recommendation, pp. 34-37. To avoid repeating many arguments set forth throughout this submission, CTA calls the FCC's attention to numerous factors that demonstrate CTA's independence and specifically Exhibit 16, Section V.A., which is incorporated herein by reference.

Corporation ("CT"), which, as of April 23, 2020, owns approximately 70.89% of the shares of CTCL.[2]

By establishing CTA as a U.S. corporation, CT demonstrated its respect for U.S. laws and jurisdiction. CT set up a legal entity in the United States that would be fully subject to the jurisdiction of the United States, because of its desire, determination and confidence to conduct business and operation in compliance with U.S. law. Specifically, CTA's establishment in the United States and subsequent application for international section 214 authorizations were legitimate and in compliance with applicable law.

As a corporation governed by the General Corporation Law of the State of Delaware, CTA's directors and management must discharge their fiduciary duties towards CTCL, the sole shareholder of CTA, in a way that maximizes shareholder return on investment. However, the fiduciary duties owed are not without limits and the subsidiary may not act in a way contrary to applicable local law. None of the shareholders of CTA, whether direct or indirect, can instruct CTA to do whatever the shareholder desires, and the company itself, its shareholders and directors/management must operate within the parameters of applicable law, conduct codes and articles of association. Serving its shareholder's (*i.e.*, CTCL) interest in maximizing return does not conflict with the public interest; instead, it is the cornerstone of modern economics for market participants to pursue their own interest while fulfilling the public interest.

CTA's shareholder CTCL is subject to rigorous legal regulation and public oversight, and must comply with the Company Law of the People's Republic of China ("PRC"), the rules and governance requirements in the HKEx Listing Rules, and the securities regulations in the U.S.,

[2] *See* Exhibit 1 for a complete description of the corporate ownership of CTA.

including the rules on the appointment of independent directors, protection of minority shareholders and public information disclosure. New York and Hong Kong are among the most rigorous capital markets in the world, and both have sophisticated investors and securities regulators to safeguard public investors' interests.

The directors and management of CTCL owe fiduciary duties towards the company and all of its shareholders, not just CT. Among its top 10 investors as of April 23, 2020 are internationally renowned institutional investors, such as Citigroup Inc.; BlackRock, Inc.; and JPMorgan Chase & Co. CTCL maintains a risk factor disclosure in its annual 20-F SEC filings which states that:

> "Accordingly, subject to our Articles of Association and applicable laws and regulations, China Telecom Group, as our controlling shareholder, will continue to be able to exercise significant influence over our management and policies …[.] The interests of China Telecom Group as our controlling shareholder could conflict with our interests or the interests of our other shareholders. As a result, China Telecom Group may take actions with respect to our business that may not be in our or our other shareholders' best interests."[3]

This type of disclosure is standard for publicly-traded companies that have a large controlling shareholder, and similar disclosures have been made by a number of other companies listed on the NYSE,[4] including U.S.-based telecommunication companies.[5] Such a disclosure is not unique to

---

[3] CTCL, Annual Report (Form 20-F) (Apr. 23, 2020), https://www.sec.gov/Archives/edgar/data/1191255/000119312520123302/d851335d20f.htm#rom851335_9.

[4] *See, e.g.,*, XG Sciences Inc., Annual Report (Form 10-K) (Apr. 29, 2020), https://www.sec.gov/Archives/edgar/data/1435375/000173112220000416/e1871_10k.htm; Jupai Holdings Limited, Annual Report (Form 20-F) (Apr. 24, 2020), https://www.sec.gov/Archives/edgar/data/1616291/000110465920050552/a20-5556_120f.htm; Biovie Inc., Annual Report (Form 10-K) (Sep. 27, 2019), https://www.sec.gov/Archives/edgar/data/1580149/000152013819000336/bivi-20190630_10k.htm.

[5] *See* T-Mobile US, Inc., Annual Report (Form 10-K) (May 21, 2020), https://www.sec.gov/Archives/edgar/data/1283699/000128369916000073/tmus12312015form10-k.htm#s02FD660242FE632F6DAFE0390B4F18A8 ("We are controlled by Deutsche Telekom, whose interests may differ from the interests of our other stockholders. … Deutsche Telekom may

CTCL and should not be taken as evidence that CTCL is subject to "exploitation, influence, and control" of the Chinese government.

In the area of corporate governance and corporate social responsibility, CTCL has been widely recognized and appreciated by the capital market. For example, CTCL was awarded "Most Honored Company in Asia" by Institutional Investor for the 9th consecutive year.[6] CTCL was awarded the "Platinum Award – Excellence in Environmental, Social and Governance" by The Asset for the 11th consecutive year.[7] In addition, CTCL was awarded "The Best of Asia – Icon on Corporate Governance" by Corporate Governance Asia for the 12th time,[8] and has received additional awards from Finance Asia including ranking as "No. 1 Best Managed Company", "No. 1 Best Investor Relations" and "No. 1 Best ESG" in China region.[9] The above-mentioned awards show that CTCL has a strong corporate governance structure and its management has not acted to

---

have strategic, financial, or other interests different from our other stockholders, including as the holder of a substantial amount of our indebtedness and as the counter-party in a number of commercial arrangements, and may make decisions adverse to the interests of our other stakeholders."); Sprint Corporation, Annual Report (Form 10-K) (May 21, 2020), https://www.sec.gov/Archives/edgar/data/101830/000010183019000022/sprintcorp201810-k.htm#s8925A97DDFA55204808914F6529AC721 ("As long as SoftBank controls us, other holders of our common stock will have limited ability to influence matters requiring stockholder approval and SoftBank's interest may conflict with ours and our other stockholders. … The interests of SoftBank may not coincide with the interests of our other stockholders or with holders of our indebtedness.").

[6] *Recognition & Awards*, CTCL, https://www.chinatelecom-h.com/en/company/awards.php?year=2019 (last accessed June 2, 2020).

[7] *The Asset ESG Corporate Awards 2019*, ASSET PUBLISHING AND RESEARCH LIMITED., https://www.theasset.com/awards/esg-awards-2019 (last accessed June 2, 2020).

[8] *China Telecom Honored with "The Best of Asia - Icon on Corporate Governance" and Awards in IR, CSR and Other Aspects*, PR NEWSWIRE ASIA LTD., https://en.prnasia.com/releases/apac/china-telecom-honored-with-the-best-of-asia-icon-on-corporate-governance-and-awards-in-ir-csr-and-other-aspects-252569.shtml (last accessed June 2, 2020).

[9] *Who Are the Best Managed Companies in China & Hong Kong?*, FINANCEASIA, https://www.financeasia.com/article/who-are-the-best-managed-companies-in-china-hong-kong/450031 (last accessed June 2, 2020).

the detriment of the company, its minority shareholders, or the commercial independence of its subsidiary, CTA.

It is important that the Commission have a full understanding of the functions of the State-Owned Assets Supervision and Administration Commission ("SASAC"). SASAC is the special governmental agency created to manage and supervise state-owned assets with the authorization from the PRC State Council. SASAC was created to preserve and increase the value of state-owned assets. As such, the core function of SASAC is to manage capital, with a focus on the economic performance and social effect of SOEs. SASAC does not have social or public management functions, and it is not in a position, nor does it have any mandate, to "exploit, influence or control" SOEs (or their domestic and overseas subsidiaries).

The law of the PRC and the central government have always required the delineation of (1) the role of the State, acting through SASAC, as the capital contributor to the SOEs; (2) the separation of government and enterprise; and (3) the differentiation and separation of the SOEs' ownership and management. In particular, SASAC's role is acting as the capital contributor, and SASAC cannot intervene in the independent management of an SOE in any way other than exercising its statutory rights as capital contributor. Specifically, SASAC evaluates the performance of an SOE and its directors/management based on the operational performance of the SOE, with the purpose of preserving and increasing the value of the state-owned assets, preventing asset leakage, and pursuing return on investment.

The creation of the SASAC to perform the capital contributor's responsibility was a key step in the process of reforming SOEs to adopt modern corporate governance structures and achieve separation between the Chinese government and SOEs. To date, nearly all of the central

SOEs have adopted a modern corporate governance structure in accordance with the PRC Company Law and relevant laws and regulations on state-owned assets. CT and CTCL similarly have adopted this modern structure. For instance, CT has a board of directors and senior management to run the company independently, with SASAC acting as the capital contributor having shareholder rights and obligations, and CTCL has a board of directors and senior management to run the company independently, with CT having shareholder rights and obligations as a shareholder of CTCL.

The Recommendation raises concerns regarding amendments to the articles of association ("AOA") of CTCL (and other SOEs) to incorporate Party building ("AOA Amendments").[10] The purpose of the AOA Amendments was to further improve the corporate governance of SOEs, standardize the relationship between party organizations and other corporate governance bodies (such as the board of directors) in corporate governance. When viewed in the broader context of SOE reform and corporate governance, such AOA Amendments have been recognized by certain investors, including foreign investors, as increasing the clarity and transparency of the role of Party organization in SOEs. Moreover, at the same time, the Chinese government emphasized that the supervision and management of state-owned assets should "focus on capital management", and the regulatory matters related to state-owned assets or SOEs were substantially cancelled or decentralized, giving SOEs more independence from the government.

[10] Recommendation, pp. 35-37.

EXHIBIT 16

A detailed response to the allegations raised in the Executive Branch Recommendation to Revoke, requesting that the Commission revoke and terminate China Telecom Americas' international Section 214 authorizations.

TABLE OF CONTENTS

I. Introduction

As directed in the Show Cause Order, China Telecom (Americas) Corporation ("CTA") responds herein to the allegations contained in the Recommendation of the Executive Branch Agencies (the "Recommendation"), filed with the Commission on April 9, 2020, seeking revocation of CTA's international Section 214 authorizations.[1] For the reasons stated below, the allegations in the Recommendation do not justify the proposed revocation.

[1] CTA notes that the Recommendation was accompanied by a classified appendix, which was not served upon CTA. Recommendation, p. 57. CTA is unable to respond at this time to any allegations that may be contained in this appendix. If the Commission does commence a proceeding to consider revocation of CTA's authorizations, it is incumbent upon the Commission to ensure that CTA has notice of *all* allegations against it and an opportunity to respond to them. 5 U.S.C. § 558(c). Due process requires that parties against whom classified information is used in a critical way be given a meaningful opportunity to respond. Although the Commission may "withhold publication of records or proceedings containing secret information affecting the national defense," 47 U.S.C. § 154(j), courts have approved agency reliance on classified information only where "the unclassified material provided to [the affected party] is sufficient to justify the [decision]." *See People's Mojahedin Org. v. U.S. Dep't of State*, 613 F.3d 220, 231 (D.C. Cir. 2010) (per curiam). The Constitution requires "that the government take reasonable measures to ensure basic fairness to the private party and that the government follow procedures reasonably designed to protect against erroneous deprivation of the private party's interests." *Al Haramain Islamic Found., Inc. v. U.S. Dep't of Treasury*, 686 F.3d 965, 980 (9th Cir. 2012). This is particularly the case where there may be a means to provide the information without implicating national security (*e.g.*, an unclassified summary or review by counsel with the appropriate security clearance). *See, e.g.*, *Al Haramain*, 686 F.3d at 1001 (finding that Office of Foreign Asset Control violated due process rights by "failing to provide constitutionally adequate notice and a meaningful opportunity to respond, and by failing to mitigate the use of classified information by, for example, preparing and disclosing an unclassified summary"). Even where unclassified information may be sufficient to support the agency's decision (which, as explained below, it is not), courts often require the government to disclose the classified information "*ex parte* and *in camera*" to a neutral adjudicator to determine whether reliance on non-disclosed classified information is appropriate. *See, e.g.*, *People's Mojahedin Org.*, 613 F.3d at 227 (noting that the court may review classified information in the administrative record); *Holy Land Found. For Relief & Devel. v. Ashcroft*, 333 F.3d 156, 164 (D.C. Cir. 2003) (noting that the International Emergency Economic Powers Act authorizes *in camera* review of classified information for decisions based on such information); *KindHearts for Charitable Humanitarian Dev., Inc. v. Geithner*, 710 F. Supp. 2d 637, 660 (N.D. Ohio 2010) (suggesting that an agency would need to provide documents for *in camera* review by counsel if the agency could not declassify adequate information to provide constitutionally adequate notice).

The Recommendation urges the Commission to take the unprecedented action of revoking the *existing* international section 214 authorizations of CTA, an American company that has operated continuously in the U.S. for more than 18 years—and to do so without any evidence that CTA violated the Communications Act or other law, or any Commission regulation. The Commission has never before revoked the international section 214 authorizations of an active, operating telecommunications company; and the Recommendation falls far short of the burden that the Commission must sustain to revoke CTA's authorizations.[2]

The Recommendation argues that CTA's authorization should be revoked based on a vague and subjective set of "factors" designed by Team Telecom. The Recommendation, however, does not even acknowledge that its proposal would terminate services to thousands of customers who rely on CTA for accessible and cost-effective service between the United States and China, the world's two largest economies. It does not explain how any business located in the two countries can communicate with each other without using "last mile" services provided by Chinese companies. Nor does it explain what exactly is unique about CTA, which uses the facilities of carriers **[BEGIN HIGHLY CONFIDENTIAL]** [redacted] **. [END HIGHLY CONFIDENTIAL]**

The Correct Legal Standard: To impose the drastic remedy of *revocation* of an existing authorization, the Commission carries the burden of showing *by clear and convincing evidence on an adjudicative record* that CTA committed "egregious misconduct" in violation of the Communications Act, the Commission's rules or orders, or the terms of CTA's section 214 authorizations.

[2] CTA reserves its right, in the event that the Commission commences an evidentiary hearing, to present additional evidence regarding the matters addressed in this Exhibit. At such a hearing, CTA must have the ability respond to any evidence or argument that may be offered against it. CTA cannot reasonably be expected to anticipate at this time all allegations and arguments that may arise during a future proceeding.

See Section II.A below. Operating from its offices in Virginia and California since 2002, CTA has consistently cooperated with U.S. government authorities; and neither the Commission nor any court has found that it has violated U.S. laws or regulations.

The Recommendation does not even mention this legal standard and, instead, asks the Commission to adopt a "fourteen-factor test," which Team Telecom developed to oppose China Mobile USA's section 214 authorization application. But that test was not adopted by the Commission in the *China Mobile* decision, is contrary to decades of FCC precedents, and rests on vaguely defined factors that invite arbitrary and capricious assessment. Those factors call for speculation (*e.g.*, "is vulnerable to," "provide opportunities for," "could result in"), which is particularly troublesome when applied to CTA—an existing section 214 authorization holder with a history of compliance with U.S. law and cooperation with U.S. government authorities. *See* Section II.B below.

CTA's Scope of Work: In the ordinary course, CTA has no access to the underlying data transmitted by its customers. Although CTA holds indefeasible rights of use ("IRUs"), CTA leases but has not constructed underlying long haul and local distribution lines in the United States. For its enterprise services, CTA provides communications and Internet-based services to its customers by leasing lines from other carriers and providing the switching, routing and related equipment and value-added services necessary to meet customer request for services.[3] For its cell services ("CTExcel"), CTA relies on services offered by **[BEGIN HIGHLY CONFIDENTIAL]** [redacted] **[END HIGHLY CONFIDENTIAL]** which in turn aggregates cell services offered by **[BEGIN HIGHLY CONFIDENTIAL]** [redacted]. [redacted] **[END HIGHLY CONFIDENTIAL]** provides end-to-end cell service within the United States. All international

[3] *See* Exhibit 6.

calls are processed through **[BEGIN HIGHLY CONFIDENTIAL]** [redacted] **[END HIGHLY CONFIDENTIAL]** which transmits the calls to Hong Kong for further routing.

For both sets of services, CTA has no access in the ordinary course to the user data transmitted by its customers. In addition, CTA's enterprise customers are generally sophisticated users that encrypt their data before ever presenting it to CTA. The scope of potential and suspected vulnerabilities enumerated in the Recommendation is inconsistent with CTA's limited business model. *See* Section III below.

CTA's Interactions with Team Telecom: The Recommendation takes issue with CTA's communication with Team Telecom on two subjects, but both of these claims are based on misinterpretations of CTA's statements. First, it claims that CTA "contradicted" itself by saying that records about its U.S. customers are stored in the United States, and then by saying that its non-U.S. affiliates have access to these same records. Because these records are stored in an electronic database, there is no contradiction in having the records be stored in the U.S. and accessible elsewhere, and the Recommendation offers no explanation of why Team Telecom could reasonably have understood otherwise. *See* Section IV.A below. Second, it claims that CTA was uncooperative in responding to inquiries about its cybersecurity policies, and speculates that CTA may have made incorrect disclosures about these policies to its customers. Quite contrary, however, CTA has always cooperated with Team Telecom and timely responded to its inquiries. CTA also had numerous policies that put a high priority on cybersecurity and customer privacy. The Recommendation offers no facts to support its hypotheses about possible misrepresentations to customers. *See* Section IV.B below.

Alleged "Exploitation, Influence, and Control" by the Chinese Government: CTA is a corporation established under U.S. law, and its management is obligated to comply with U.S.

law. CTA operates as an autonomous commercial enterprise, and it is responsible to its parent company for its commercial performance. CTA locally hires and evaluates its own employees, and trains its employees in their compliance obligations under U.S. law. There is no basis for the suggestion in the Recommendation that CTA might be compelled to pursue some other goal. *See* Section V.A below.

Alleged Forced Compliance with Requests from the Chinese Government: The application of Factors 3–12 in the Recommendation's "fourteen-factor" test rests on speculation that CTA "will be" forced to comply with Chinese government requests pursuant to the 2017 Cybersecurity Law. The Chinese Cybersecurity Law, by its terms, only applies to "the construction, operation, maintenance, and use of networks … *within the territory of the People's Republic of China*." The Cybersecurity Law is inapplicable by its terms to CTA's operations. *See* Section V.B below.

Alleged Threat of Internet Disruption: The Recommendation's allegation of "hijacking" the internet also does not justify revoking CTA's authorizations. The Recommendation asks the Commission to conclude that CTA and CTA's parent, China Telecom Corporation Limited ("CTCL"), have intentionally misrouted internet traffic though China, noting 10 such occasions over 10 years. Misrouting incidents are a common occurrence in the global internet, and can occur due to errors by operators of other networks that use CTA and CTCL's global backbone, with no action or error by CTA. To put these 10 events in 10 years into perspective, there were 1,197 routing incidents in April 2020 alone involving 967 networks, of which 269 were U.S. networks. *See* Section V.D below.

Subjective Judgment of "Trustworthiness": Factors 1–2 and 13–14 in the Recommendation inherently rely on a subjective judgment: that the Executive Branch has decided CTA is not

"trustworthy" because CTA purportedly violated its Letter of Assurance ("LOA") with Team Telecom in two respects. But neither claim is correct.

The Recommendation identifies no specific problem with the "practicable measures" used by CTA "to prevent unauthorized access to, or disclosure of the content of, communications or U.S. Records, in violation of any U.S. Federal, state, or local laws or of the commitments set forth" in the 2007 LOA. Rather, it argues that because CTA did not until recently have a single, consolidated written cybersecurity policy—which is *not* required by the language of the 2007 LOA nor by any federal or state law—it has failed to take "practicable" steps to ensure security. In fact, CTA has always placed a high value on network security, as it was required to do. *See* Section V.E.1 below.

The Recommendation also alleges that CTA violated the LOA by failing to give Team Telecom notice before it requested two International Signaling Point Codes (in addition to the one it already had at the time of signing the LOA). The most reasonable interpretation of the LOA is that CTA is only required to give Team Telecom notice of substantive applications to the FCC, not ministerial requests for allocation of numbering resources. Therefore, CTA did not violate its LOA. However, even if the LOA were interpreted as the Recommendation suggests, this would at most be a trivial, technical violation, not "egregious" misconduct of the type that could justify a revocation. *See* Section V.E.2 below.

Possibility of Mitigation: The Recommendation also summarily dismisses the possibility of mitigation. Because the fourteen-factor test relies heavily on speculation about future harms—rather than any evidence of past or current "egregious misconduct"—the Commission must decide whether there is a remedy short of revocation that would foreclose the hypothetical risks suggested

by the Recommendation, none of which have actually occurred, while preserving the services used by thousands of CTA customers. *See* Section V.E.3 below.

II. The Commission Should Not Revoke Section 214 Authorizations Except on Proof of a Violation of Relevant Statutes or Regulations

Until this proceeding, the Commission had only revoked existing international section 214 authorizations held by defunct or inactive companies. In these cases, the Commission did not have to consider the interests of an ongoing telecommunications company, its hundreds of employees, and its thousands of customers. And while section 214 contains no provisions governing revocation of an authorization—and does not even mention the concept of revocation—the law in analogous circumstances is clear: revocation requires a showing *by clear and convincing evidence* that (1) CTA violated the Communications Act, the Commission's rules or orders, or the terms of CTA's section 214 authorizations, and (2) that such a violation is of an egregious nature.

The Executive Branch agencies do not acknowledge this precedent, but instead urge the Commission to consider the same 14 factors in this case as they considered in their recommendation to deny China Mobile's section 214 application in 2018.[4] Although the Commission mentioned some of Team Telecom's factors in its *China Mobile Order*,[5] the Commission did not expressly incorporate the Team Telecom analysis into its decision.[6]

---

[4] Recommendation, pp. 13-14, *citing* Redacted Executive Branch Recommendation to Deny China Mobile International (USA) Inc.'s Application for an International Section 214 Authorization, FCC No. ITC-21420110901-00289, at 6-7 (filed July 2, 2018), https://licensing.fcc.gov/myibfs/download.do?attachmentkey=1444739.

[5] *China Mobile Order*, 34 FCC Rcd 3361, 3368 ¶ 14 n.46, 3367 ¶ 12, and 3374 ¶ 26 (2019) ("*China Mobile*").

[6] *Id.* at 3365-66 ¶ 8.

The Recommendation argues that the Commission should apply the same criteria when considering revoking CTA's existing section 214 authorizations as it did to deny China Mobile's application for a *new* authorization.[7] It claims that the same factors should govern because "Section 214(a) directs the Commission to act when 'present' or 'future' interests are concerned, and to determine whether the public convenience and necessity 'require' the carrier's services[.]"[8] Its recommended approach, however, would depart from decades of precedents, inviting arbitrary and capricious decision-making and threatening CTA's constitutional rights.

A. Revocation Requires a Showing, by Clear and Convincing Evidence, of Egregious Misconduct.

"[R]evocation of an FCC license is governed, at the agency level, by the 'clear and convincing' standard of proof …."[9] While section 214 contains no provision on, and does not even mention, revocation, the Communications Act requires, in the analogous context of revocation of station licenses and construction permits, that "both the burden of proceeding with the introduction of evidence and the burden of proof shall be upon the Commission."[10]

In addition, the Commission's *Second Foreign Participation Order*, upon which the Recommendation relies extensively, explicitly states that the Commission "may impose additional

---

7 Recommendation, pp. 13, 15-16.

8 Recommendation, p. 13.

9 *Sea Island Broadcasting Corp. of S.C. v. FCC*, 627 F.2d 240, 244 (D.C. Cir. 1980).

10 47 U.S.C. § 312(d); *see* 47 C.F.R. § 1.91(d).

conditions on a Section 214 authorization or revoke the authorization *in cases of adjudicated misconduct*."[11] The Commission subsequently clarified that "adjudicated misconduct" means "a violation of the terms of an authorization, the Act, or a Commission rule or order."[12] In *Marpin*, the Commission rejected a theory that it may take adverse actions against a U.S. carrier's section 214 authorization "based solely on the misconduct of its foreign affiliate"; to the contrary, there must be evidence that the U.S. carrier itself "engaged in … 'adjudicated misconduct.'"[13] If the Commission seeks to revoke the section 214 authorization as a remedy, Commission precedents additionally require that the adjudicated misconduct be of an "egregious" nature.[14]

The Commission's precedents for revoking section 214 authorizations demonstrate its conscientiousness in applying these precedents before imposing the drastic remedy of revocation. All but one of these revoked the authorizations of defunct or dissolved carriers that failed to even

---

[11] 12 FCC Rcd 23891, ¶ 295 (1997) (emphasis added).

[12] *Marpin Telecoms and Broadcasting Company Limited v. Cable & Wireless, Inc.*, 18 FCC Rcd 508, 515 (2003), denying recon. of 17 FCC Rcd 7601 (2002).

[13] *Id.*

[14] *See Protecting Consumers from Unauthorized Carrier Changes & Related Unauthorized Charges*, 33 FCC Rcd 5773 (2018) ("[W]e will consider initiating proceedings to revoke Section 214 operating authorization in cases of 'egregious misconduct and the demonstrated harm to consumers from the apparent violations.'"); *Sandwich Isles Commc'ns, Inc.*, 31 FCC Rcd 12947 (2016) (issuing order to show cause why the Commission should not revoke the carrier's section 214 authorizations "in light of [its] egregious misconduct and the demonstrated harm"); *Int'l Settlements Policy Reform*, 27 FCC Rcd 15521, ¶¶ 61–62 (2012) (finding that because revocation of a section 214 authorization "is a severe remedy … such a remedy should be reserved for cases of sustained circuit disruption or other egregious behavior"); *FCC Enf't Advisory*, 26 FCC Rcd 16411, 16412 (2011) ("In egregious cases a carrier could face … even revocation of its section 214 authorization to operate as a carrier.").

respond to government notices despite multiple attempts—a failure which constitutes a clear violation of the terms for maintaining a carrier's section 214 authorization.[15] The only other revocation case involved a group of inactive carriers that, in addition to failing to respond to the Commission's Order to Show Cause, committed "egregious actions and blatant violations of [the Commission's] rules and the [Communications] Act."[16] All the precedents are therefore consistent

[15] *Wypoint Telecom, Inc. Termination of International Section 214 Authorization*, Order, 30 FCC Rcd 13431 (2015) (revoked the section 214 authority of a carrier upon the recommendation of Team Telecom for failure to abide by the terms of a letter of assurance and FCC rules following the carrier's dissolution and failure to respond to government requests); *ACT Telecommunications, Inc. Termination of International Section 214 Authorization*, Order, 31 FCC Rcd 188 (2016) (revoked section 214 authority upon the recommendation of Team Telecom for failure to abide by the terms of a letter of assurance and FCC rules following the carrier's failure to respond to government requests); *Ocean Technology Limited Termination of International Section 214 Authorization*, Order, 31 FCC Rcd 357 (2016) (same); *JuBe Communication, LLC Termination of International Section 214 Authorization*, Order, 31 FCC Rcd 7096 (2016) (same); *Redes Modernas de la Frontera SA de CV Termination of International Section 214 Authorization*, Order, 31 FCC Rcd 12709 (2016) (same); *IP to Go, LLC Termination of International Section 214 Authorization*, Order, 31 FCC Rcd 12713 (2016) (same); *WX Communications Ltd. Termination of International Section 214 Authorization*, Order, DA 19-130 (IB 2019) (same); *Space Net LLC Termination of International Section 214 Authorization*, Order, DA 19-143 (IB 2019) (same); *Cablemas International Telecomm, LLC Termination of International Section 214 Authorization*, Order, DA 19-192 (IB 2019) (same); *Air Channel Communications, Inc. Termination of International Section 214 Authorization*, Order, DA 19-210 (IB 2019) (same); *StarVox Communications, Inc. and Capital Telecommunications, Inc. Termination of International Section 214 Authorization*, Order, DA 19-243 (IB 2019) (same); *Angel Americas, LLC and Angel Mobile, Inc. Termination of International Section 214 Authorization*, Order, DA 19-1150 (IB 2019) (same).

[16] *CCN, Inc., et al.*, 13 FCC Rcd 13599 (1998). That inactive carrier group was the subject of over 1,400 customer complaints to the Commission, in a period of four years, that they engaged in illegal and fraudulent practices of changing consumers' carriers without the consumers' knowledge or authorization, "forg[ing] or falsif[ying] letters of agency" to the local exchange carriers, billing consumers for long distance calls that they did not place, etc. *Id.* at 13601. Commission staff determined that the carriers had ceased operating at least a year before the revocation order was issued. *Id.* at 13600.

with the long-standing requirement that the Commission must prove, by clear and convincing evidence, that the complained-off carrier has engaged in egregious violation of the Communications Act, the Commission's rules or order, or the terms of its section 214 authorizations.

B. The Executive Branch's Novel "Fourteen-Factor" Test Violates Commission Precedent.

The revocation of an existing authorization is quite a different matter from the denial of an application. In the *China Mobile* decision, the Commission emphasized that the applicant had the burden of "demonstrating how grant of its international section 214 application would serve the public interest, convenience, and necessity."[17] By contrast, as shown above, in a revocation proceeding the Commission must find "clear and convincing evidence" of egregious misconduct.[18] In addition, the substantive issues in a revocation proceeding are different than those in a licensing proceeding, because revocation of an existing authorization will have an effect on existing customers. By definition, an applicant for a new section 214 authorization does not have any existing customers whose service would be affected by a denial of the application. CTA, on the other hand, has numerous customers who, at a minimum, would be put to the inconvenience and disruption of having to find replacement services if its section 214 authorizations were revoked. Dismantling and replacing communications service can be expensive, time consuming and difficult. Even assuming that all these customers could find other providers, there is no guarantee they will be able to find services that offer the same combination of features at the same price. Congress recognized that disruption of service to existing customers is potentially contrary to the public interest when it prohibited carriers from discontinuing or reducing services under FCC jurisdiction unless the

---

[17] *China Mobile*, 34 FCC Rcd at 3366, ¶ 9.

[18] *See* 47 C.F.R. § 1.91(d).

Commission determines "that neither the present nor future public convenience and necessity will be adversely affected thereby."[19]

The Recommendation suggests reversing the burden of proof to require CTA to prove that "the public interest would be served by the [retention] despite national security and law enforcement risks identified by the Executive Branch."[20] It also argues that "the Commission should … apply the same deference [as it does with respect to a pending application] to the Executive Branch's expertise with respect to any national security and law enforcement concerns associated with an existing international Section 214 authorization."[21] As discussed above, however, revocation presents different public interest considerations than pending applications, and so precedent from application cases stating that the Commission would defer to Executive Branch expertise is not relevant in this context. And, in any event, "deference" cannot mean "abdication" — the Commission has a statutory responsibility to weigh the public interest, convenience, and necessity, and cannot side-step that duty by relying unquestioningly on the findings of other agencies.[22] The Commission must conduct its own, independent analysis of the relevant facts.

Adoption of the Executive Branch's "fourteen-factor" test would be a decided break from the Commission's long-standing practice on revoking section 214 authorizations. Aside from factor 1 ("[w]hether the carrier has a past criminal history")—which the Executive Branch admits that

---

[19] 47 U.S.C. § 214(a).

[20] Recommendation, p. 13.

[21] Recommendation, p. 13.

[22] *See, e.g.*, *City of Tacoma, Washington v. FERC*, 460 F.3d 53, 76 (D.C. Cir. 2006) (stating that "the action agency [Federal Energy Regulatory Commission] must not blindly adopt the conclusions of the consultant agency …. [T]he ultimate responsibility for compliance [] falls on the action agency."); *Former Employees of Int'l Bus. Machines Corp. v. U.S. Sec'y of Labor*, 29 C.I.T. 1360, 1382 (2005) (holding that "the [Labor Department] must reach its own conclusions, based on its own thoughtful, thorough, independent analysis of all relevant record facts.").

CTA does not have—none of the other factors is remotely relevant to the carrier's violation of the Communications Act, the Commission's rules or order, or the terms of its section 214 authorizations. They rely on a highly subjective assessment of "trustworthiness" and speculation about the carrier's "vulnerab[ilities]," what "could" happen, and what the carrier's operations "provide opportunities for"—factors that have nothing to do with "misconduct" and that are not even susceptible of "clear and convincing" proof. The Commission should not depart from its precedents and follow this *ad hoc* path.[23]

Further, the 14-factor test described in the Recommendation invites arbitrary and capricious decision-making, is unconstitutionally vague, and threatens a taking of CTA's authorization without due process of law. The arbitrariness and vagueness of the factors give the agencies virtually unlimited discretion to blackball any telecommunications carrier from the U.S. market based on political or ideological considerations, regardless of whether the carrier's operations pose any actual threat to U.S. national security. For example, Factors 4 and 5 are based solely on the fact of a carrier's foreign ownership, allowing the Executive Branch to target any foreign country it desires.[24] Factors 8 through 12 ask "[w]hether the carrier's operations within the United States provide opportunities for the carrier *or other actors*" to engage in particular conduct.[25] No matter what steps a carrier takes to protect its network and prevent improper activities, it is never possible for

---

[23] *See Ramaprakash v. FAA*, 346 F.3d 1121, 1124–25 (D.C. Cir. 2003) (stating that "review under the APA is highly deferential, but agency action is arbitrary and capricious if it departs from agency precedent without explanation.") (citations omitted). *See also Pacific N.W. Newspaper Guild, Local 82 v. NLRB*, 877 F.2d 998, 1003 (D.C. Cir. 1989) (stating that "the core concern underlying the prohibition of arbitrary or capricious agency action" is that agency "ad hocery" is impermissible).

[24] The Commission has stated expressly that ownership of a carrier by a foreign government is not, by itself, ground for denying a section 214 application. *China Mobile*, 34 FCC Rcd at 3371, ¶ 20. *A fortiori*, that cannot be a sufficient basis for revoking an authorization.

[25] Recommendation, pp. 14-15 (emphasis supplied).

any carrier (even a U.S.-owned carrier) to eliminate the possibility that "other actors" might engage in misconduct; thus, these five factors are inherently impossible for any carrier to satisfy. Combined with the subjective, vague and open-ended nature of several of the other factors, this leads to a "test" that allows the Executive agencies unlimited discretion to decide what companies they want to paint as threats to national security. It would be arbitrary and capricious for the Commission to endorse a Recommendation based on such an amorphous, shifting, and opaque standard.

C. The *China Mobile* Rationale Cannot Be Extended to Revocation Proceedings.

The Order to Show Cause in this proceeding cites the Commission's *China Mobile Order* as part of the basis for considering revocation of CTA's authorizations.[26] The Commission denied China Mobile USA's application for section 214 certification on the ground that "China Mobile USA is vulnerable to exploitation, influence, and control by the Chinese government. We also find that, in the current security environment, there is a significant risk that the Chinese government would use the grant of such authority to China Mobile USA to conduct activities that would seriously jeopardize the national security and law enforcement interests of the United States."[27]

"Exploitation, influence, and control" is not a reasonable standard to apply in a license revocation proceeding. When an agency proposes to subject a party to "drastic" sanctions, such the revocation of a license, it must do so based on standards that "a regulated party acting in good faith would be able to identify, with 'ascertainable certainty[.]'"[28] An agency may not penalize a

---

[26] *See China Telecom (Americas) Corporation*, GN Docket No. 20-109 et al., Order to Show Cause, DA 20-448, ¶¶ 7, 9, 10 (Apr. 24, 2020) ("*Order to Show Cause*").

[27] *China Mobile*, 34 FCC Rcd at 3365-66, ¶ 8. The *China Mobile* decision was a case of first impression, and was not appealed, so no court has had an opportunity to review the decisional criteria used by the Commission in that case.

[28] *Gen. Elec. Co. v. EPA*, 53 F.3d 1324, 1329 (D.C. Cir. 1995); *citing Diamond Roofing Co. v. OSHRC*, 528 F.2d 645, 649 (5th Cir. 1976).

party for failing to comply with a standard that is so vague or subjective that the party cannot reasonably know what conduct will comply with it. As the D.C. Circuit explained in reviewing the NLRB's interpretation of a regulation governing union dues —

> [I]f the Board's order is to be enforced it must be based on an adequate explanation of why the union's conduct violated the law. If the Board wishes to draw an interpretative distinction between anticipatable and unpredictable charges, it must do so under a legal theory that permits a union reasonably to "predict" whether a particular practice will be lawful or not. Otherwise, we sanction impermissible "ad hocery" on the part of the Board which is the core concern underlying the prohibition of arbitrary or capricious agency action.[29]

The criteria discussed in the *China Mobile* decision were largely *ad hoc*, and focused primarily on the state of international relations between the United States and China. Obviously, it is impossible for any company to predict what foreign country may become involved in future political disputes with the United States, or to modify its behavior in a way that will alter the state of international relations. The Commission may only revoke a company's authorization based on a standard that gives the company notice of the conduct required of it, and an opportunity to conform to that standard.

Most troubling, the Commission acknowledged that it relied heavily on "reports [that] do not specifically mention China Mobile USA (which currently holds no Commission authorizations), but … that … highlight concerns with actions by the Chinese government and Chinese state-owned enterprises."[30] The Commission discounted all evidence that the applicant offered about its own practices and operations, instead basing its public interest determination on purported evidence about the conduct of other companies:

> [W]e find persuasive in the current security environment the argument that there is a significant risk that the Chinese government would use China Mobile USA to

---

[29] Pacific N.W. Newspaper Guild, Local 82 v. NLRB, 877 F.2d 998, 1003 (D.C. Cir. 1989).

[30] *China Mobile*, 34 FCC Rcd at 3373, ¶ 24.

> conduct activities that would seriously jeopardize the national security interests and law enforcement activities of the United States. Although *there is no public record information that the Chinese government has used China Mobile or China Mobile USA for these purposes to date*, there is clear evidence in the public record that the Chinese government has used *other* state-owned Chinese companies to act against U.S. interests. Given the Chinese government's ability to similarly exert influence and control over China Mobile and China Mobile USA and the Executive Branch agencies' assessment that the Chinese government would use these entities for activities counter to U.S. interests if the opportunity arises, we find this information relevant to our public interest review of the application.[31]

It would be arbitrary, capricious, and irrational to revoke an existing license on this basis. A licensee must be given notice of the standards with which it is required to comply, and cannot be penalized for the behavior of other, unknown third parties.

At a minimum, the Administrative Procedure Act requires that, before a license is revoked, the licensee be given an "opportunity to demonstrate *or achieve compliance with* all lawful requirements."[32] Here, the Commission has provided no standard or guideline by which CTA could determine what it needs to do to be in compliance with "all lawful requirements." Without some objective criteria against which its compliance can be assessed, the Commission cannot lawfully revoke CTA's authorizations.

III. CTA's Operations in the United States

CTA has been doing business in the United States for almost two decades. In 2001, CTA was incorporated in Delaware under the name "China Telecom USA." In 2002, it established its headquarters in Herndon, Virginia, where it maintains its operations today. In 2007, China Telecom USA changed its name to "China Telecom (Americas) Corporation". CTA expanded its portfolio of services to include Mobile Virtual Network Operator ("MVNO") services in 2015 under the "CTExcel" brand name, reselling mobile services directly to retail customers.

---

[31] *China Mobile*, 34 FCC Rcd at 3376, ¶ 30 (emphasis supplied).

[32] 5 U.S.C. § 558(c)(2) (emphasis supplied).

CTA is a commercial, for-profit enterprise that has worked to expand telecommunications opportunities in the United States, focusing primarily on communications between the U.S. and China. Although CTA holds IRUs, CTA leases but has not constructed underlying long haul and local distribution lines in the United States. CTA provides communications and Internet-based services to its customers by leasing lines from other carriers and providing the switching, routing and related equipment and value-added services necessary to meet customer request for services as detailed in Exhibit 6. CTA provides value to both its U.S. and Chinese enterprise customers that require connectivity between the countries. For U.S. enterprise customers that seek services connecting to China, CTA adds value through the resources that CTA can access through its foreign affiliates, providing technical support in English, billing for service in U.S. dollars, and using contracts governed by U.S. law. For its Chinese customers that have operations in the United States, CTA provides a bilingual service team and connects the customer to the United States. As with Chinese enterprise customers, CTA's primary value to MVNO users is providing a Chinese language service team.

CTA currently has 224 employees in the United States, of whom 72 are U.S. citizens and 53 are U.S. permanent residents. Many of these U.S. citizens and permanent residents are long-term employees of CTA, with 40 having worked for CTA for five years or more; 29 having worked for CTA for seven years or more, and 20 having worked for CTA for 10 or more years.

The Recommendation contains several general background sections that purport to provide factual support for the specific grounds relied upon for proposing revocation of CTA's authorizations.

First, pages 2 to 7 of the Recommendation argue that "[t]he national security environment has changed significantly since 2007[.]" This section details U.S. government concerns about the

Government of China. CTA's management has no knowledge of any of the allegations recited in this section, but nothing in this section relates directly to CTA or even to its corporate parent and affiliates. As explained in Section II above, the Commission should not revoke any authorizations held by CTA based on the state of international relations between the United States and China, but only (if at all) based on facts and conduct specifically related to CTA. Further, the Recommendation's lengthy discussion of "economic espionage" and "trade secret theft" allegations is entirely irrelevant to CTA, because (as will be discussed further below) the nature of CTA's business in the U.S. simply does not provide the opportunity for any such activities. Nothing in this section, or anywhere else in the Recommendation, disputes that CTA has complied with U.S. law — a fact that has *not* changed since the company's inception.

Second, the Recommendation's narrative about CTA's products and services appears to exaggerate the scope and scale of CTA's operations in the United States. Pages 7 to 12 purport to describe the "full suite of services" offered by CTA, including common carrier communications services offered pursuant to its section 214 authorizations, other services that the Recommendation describes as being in a "grey area," and non-communications services that even the Recommendation concedes do not require any Commission authorization. Rather than provide factual and technical description of these services, however, the Recommendation quotes marketing materials.[33] A more complete description of CTA's current services is contained in Exhibit 6. The Recommendation never mentions that CTA leases but has not constructed underlying long haul and local distribution lines in the United States. CTA obtains access to customer premises in the U.S.

[33] For example, the Recommendation states that CTA "targets" its MVNO service "to more than four (4) million Chinese Americans, two (2) million Chinese tourists visiting the United States annually, 300,000 Chinese students at U.S. colleges, and more than 1,500 Chinese businesses in the United States." Recommendation, pp. 8-9. Those figures represent the *potential* market, not the actual scale of CTA's service, which serves only a small fraction of these numbers at present.

by purchasing dedicated transmission services from domestic carriers, or a customer may arrange for a third party carrier to deliver the customer's traffic to CTA's POP. For international circuits, CTA typically acts as a sales channel for the transmission services provided by CTA's overseas affiliates. It also obtains global network capacity from other international telecommunications carriers. In short, CTA's operations are no different than the typical range of services offered by the U.S. affiliates of other foreign telecommunications carriers.

CTA markets the majority of services to U.S. businesses that need to transmit data to and from China, to the U.S. offices of Chinese businesses; and to other telecommunications carriers. U.S. businesses generally buy services from CTA mostly for their circuit needs to China (or sometimes other East Asian destinations), not primarily for their domestic U.S. traffic or circuits to other continents. The information that CTA collects from these customers is what is needed to provision and bill for the services provided to them, such as billing contact and address, location of the service, price of service, and type of service (*i.e.*, physical location of where the service will be installed/used, which may differ from the billing address). Because CTA depends on other carriers to implement services both in the U.S. and abroad, the information CTA collects from customers must be shared with those underlying carriers in order for the customer to receive the service. In China, CTA shares the same information with its affiliates, who act as the service providers in China. If a customer chooses to order the same type of service from a U.S.-owned telecommunications carrier, that carrier would have to collect the same basic information – *and provide the same information to a Chinese carrier to provide the foreign end of the circuit* – as CTA does.

The Recommendation incorrectly asserts that CTA could "provide facilities-based mobile wireless services using its own network facilities instead of reselling mobile services as it currently

does as an MVNO … without seeking further FCC approvals under Section 214."[34] CTA is ineligible to hold a common carrier radio license under Section 310(b)(3) of the Communications Act, 47 U.S.C. § 310(b)(3), because all of its stock is owned by CTCL", a corporation organized under foreign law, so it cannot offer facilities-based mobile services.

IV. Executive Branch Allegations that CTA's Conduct Shows a Lack of Trustworthiness Are Inaccurate and Misleading

The Recommendation asserts that CTA made tardy and misleading statements to Team Telecom, that it says "call[] its trustworthiness into question."[35] "Trustworthiness," like many of the other factors proposed in the Recommendation, is inherently subjective, and CTA cannot possibly respond to claims about what the Executive Branch agencies believe or conclusions they reached based on this subjective standard. However, CTA can, and does, show below that the factual allegations in the Recommendation are inconsistent with the history of interactions between CTA and Team Telecom and the actual terms of the 2007 LOA between CTA and Team Telecom. The Recommendation's claims of inaccurate and untimely statements are not justified by the facts.

A. CTA's Statements to Team Telecom Regarding Storage of U.S. Records Were Both Accurate and Consistent with Its LOA Obligations.

The Recommendation is based on a misinterpretation of CTA's statements about storage of and access to U.S. Records. It claims that these alleged misrepresentations indicate CTA's untrustworthiness, and are a ground for recommending the revocation of CTA's international section 214 authorizations.[36] Actually, CTA's statements to Team Telecom about its U.S. records were

[34] Recommendation, p. 12.

[35] Recommendation, p. 17.

[36] Recommendation, p. 26.

accurate at the times the statements were made, and there were no contradictions or misrepresentations to Team Telecom.

The Recommendation claims two "contradictions," neither of which is real.

First, it claims that CTA's 2019 statement that "[b]eginning in May 2013, … U.S. records *were available to* [CTA's] non-[U.S.] affiliates abroad[,]" contradicts its January 2016 statement that "its U.S. records were *kept at* its data center in California."[37] But there is not even any apparent contradiction between these two statements. Electronic records can be "kept" at one location and simultaneously be "available" in other locations. The allegation of a contradiction makes no sense, unless Team Telecom unreasonably believed in 2016 that CTA was still keeping all of its business records on paper in file cabinets.

Nor was there any contradiction in fact. CTA's January 2016 letter to Team Telecom simply did not address *access* to U.S. Records by its affiliates, although it did disclose that **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]** In contrast, the April 2019 submission to Team Telecom states only that such records "were available" to CTA's non-U.S. affiliates after May 2013 and makes no affirmative statements about where such U.S. Records are stored.

[37] Recommendation, p. 19, *citing* Recommendation Exhibit 103 at EB-2111-2112 and Recommendation Exhibit 125 at EB-2784 (emphasis supplied).

Second, the Recommendation claims that, "Until April 2019, [CTA] did not inform Team Telecom that other corporate entities—[CTA's] Parent Entity and Chinese affiliates—would have access to [CTA's] U.S. records."[38] In fact, CTA's overseas affiliates have *always* had access to records about CTA's U.S. services in some form, because that information is necessary for the affiliates to provision international circuits used to serve U.S. customers. And, as the correspondence between CTA and Team Telecom shows, although CTA was not under any formal obligation to do so under the LOA, CTA did inform Team Telecom on at least two occasions before April 2019 that access was being provided to CTA affiliates. Initially, CTA informed Team Telecom in a September 2014 meeting that **[BEGIN CONFIDENTIAL]** [redacted].[39] **[END CONFIDENTIAL]**Then, CTA informed Team Telecom in December 2018 of the U.S. Records Security Agreement with its parent CTCL that governs access to U.S. Records, including by CTA's non-U.S. affiliates.[40]

[38] Recommendation, p. 21.

[39] Recommendation Exhibit 125 at EB-2783.

[40] Recommendation Exhibit 36 at EB-590 (introducing the U.S. Records Security Agreement); Recommendation Exhibit 36 at EB-624. **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]** *See* Recommendation Exhibit 96 at EB-2002. **[BEGIN CONFIDENTIAL]** [redacted]. **[END CONFIDENTIAL]** *See* Recommendation, p. 18. **[BEGIN CONFIDENTIAL]** [redacted]. **[END CONFIDENTIAL]**

The Recommendation does not identify any document in which CTA made any representation to Team Telecom that its records would *not* be accessible by its affiliates for ordinary business purposes. It would have been impractical for CTA to agree to such a provision: Any suggestion that CTA would (or could) make such a commitment ignores the reality of how customers obtain service in the international telecommunications marketplace. ***No carrier, regardless of its ownership, could provide international communications services from the United States without sharing information about those services with a foreign carrier at the other end of the circuit.***

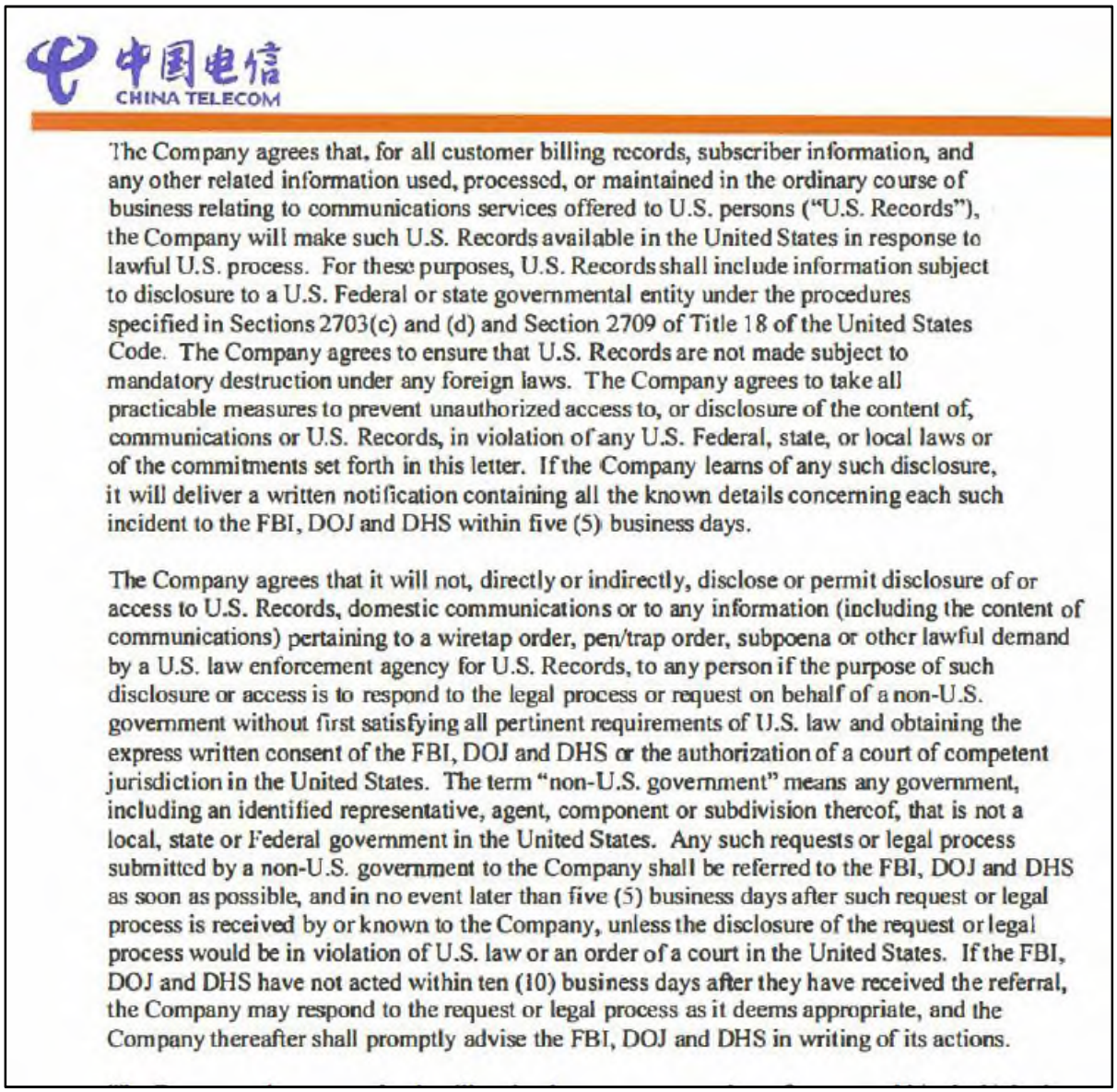
1. History of CTA's Interactions with Team Telecom

On July 17, 2007, at the time that ownership of CTA transferred from China Telecommunications Corporation ("CT") to its subsidiary, CTCL, CTA and Team Telecom entered into a LOA.[41] The 2007 LOA focused on ensuring the traditional requirement that U.S. law enforcement would have access to CTA's subscriber information for properly authorized wiretaps, pen/traps, or other lawful demands. As relevant here, CTA also agreed not to destroy its subscriber records and to take "all practicable measures to prevent unauthorized access to, or disclosure of, the content of its subscriber records in violation of any U.S. Federal, state, or local laws or the commitments set forth in this letter." The only applicable "commitment[] set forth in this letter" was a prohibition on release of data to a foreign government without first providing notice to relevant U.S. agencies. Specifically, the LOA (in relevant part) provided:[42]

---

[41] Recommendation Exhibit 1 at EB-1.

[42] Recommendation Exhibit 1 at EB-2.



中国电信
CHINA TELECOM

The Company agrees that, for all customer billing records, subscriber information, and any other related information used, processed, or maintained in the ordinary course of business relating to communications services offered to U.S. persons ("U.S. Records"), the Company will make such U.S. Records available in the United States in response to lawful U.S. process. For these purposes, U.S. Records shall include information subject to disclosure to a U.S. Federal or state governmental entity under the procedures specified in Sections 2703(c) and (d) and Section 2709 of Title 18 of the United States Code. The Company agrees to ensure that U.S. Records are not made subject to mandatory destruction under any foreign laws. The Company agrees to take all practicable measures to prevent unauthorized access to, or disclosure of the content of, communications or U.S. Records, in violation of any U.S. Federal, state, or local laws or of the commitments set forth in this letter. If the Company learns of any such disclosure, it will deliver a written notification containing all the known details concerning each such incident to the FBI, DOJ and DHS within five (5) business days.

The Company agrees that it will not, directly or indirectly, disclose or permit disclosure of or access to U.S. Records, domestic communications or to any information (including the content of communications) pertaining to a wiretap order, pen/trap order, subpoena or other lawful demand by a U.S. law enforcement agency for U.S. Records, to any person if the purpose of such disclosure or access is to respond to the legal process or request on behalf of a non-U.S. government without first satisfying all pertinent requirements of U.S. law and obtaining the express written consent of the FBI, DOJ and DHS or the authorization of a court of competent jurisdiction in the United States. The term "non-U.S. government" means any government, including an identified representative, agent, component or subdivision thereof, that is not a local, state or Federal government in the United States. Any such requests or legal process submitted by a non-U.S. government to the Company shall be referred to the FBI, DOJ and DHS as soon as possible, and in no event later than five (5) business days after such request or legal process is received by or known to the Company, unless the disclosure of the request or legal process would be in violation of U.S. law or an order of a court in the United States. If the FBI, DOJ and DHS have not acted within ten (10) business days after they have received the referral, the Company may respond to the request or legal process as it deems appropriate, and the Company thereafter shall promptly advise the FBI, DOJ and DHS in writing of its actions.

After entering into the 2007 LOA, CTA complied with its obligations under the LOA, including providing notifications to Team Telecom when necessary. Although not obligated to do so under the LOA, CTA also informed Team Telecom in 2014 that **[BEGIN CONFIDENTIAL]** [redacted]. **[END CONFIDENTIAL]** During that time, the records were always available to U.S. law enforcement agencies as required under the

LOA. In January 2016, this information was formally provided to Team Telecom by letter.[43] That letter stated: **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]** It also noted that CTA discussed this with Team Telecom during a meeting with outside counsel in 2014. Team Telecom raised no questions **[BEGIN CONFIDENTIAL]** [redacted]. **[END CONFIDENTIAL]**

On September 13, 2017, **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]** reached out to CTA by email to introduce himself as the new Team Telecom contact covering "all matters" relating to the 2007 LOA.[44] Consistent with CTA's understanding of the commitments made in the LOA, and indicating that Team Telecom and **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]** understood the LOA in the same way as CTA, **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]** set out what he understood to be the operative terms of the 2007 LOA as follows:[45]

> 1) Copies of U.S. Records, as defined in the LOA, remain available in the United States in response to lawful U.S. process;
>
> 2) To date, there has been no unauthorized access to, or disclosure of the content of communications or U.S. Records in violation of U.S. law or the commitments set forth in the LOA; [and]
>
> 3) To date, China Telecom has not, directly or indirectly, disclosed or permitted the disclosure of or access to U.S. Records, domestic communications, or any information (including the content of communications) pertaining to a wiretap, pen/trap order, subpoena or lawful demand by a U.S. law enforcement agency for U.S. Records, to any person for the purpose of responding to the legal process or request on behalf of a non-U.S. government; or, if

[43] *See* Recommendation Exhibit 125 at EB-2783.

[44] *See* Recommendation Exhibit 91 at EB-1979.

[45] Recommendation Exhibit 91 at EB-1979-80.

> such disclosures were made, proof that such requests or legal process was submitted to the USG Parties, unless such referral was in violation of U.S. law or an order of a court in the United States[.]

CTA confirmed its compliance, repeating back the language quoted above.[46] Again, Team Telecom raised no questions about access to CTA records by CTA's Chinese affiliates.

In April 2018, members of Team Telecom met with CTA again to review its compliance with the 2007 LOA. For the first time, Team Telecom asked questions at that meeting about CTA's cybersecurity practices. On June 13, 2018, **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]** wrote to CTA thanking CTA for hosting the April meeting, and seeking to confirm Team Telecom's "understand[ing] that [CTA] continues to make available in the United States U.S. Records as defined in the LOA[.]"[47] He also asked several questions about how CTA defended its networks, including tools used and how those tools were procured. Apparently recognizing that CTA's affiliates in China had access to CTA records, **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]** asked CTA whether Chinese security agencies had engaged in any "inspections" of CTA's operations, specifically including virtual private networks offered by CTA between the U.S. and China.[48]

Following several exchanges between counsel and Team Telecom, CTA provided an initial response to Team Telecom's letter on October 1, 2018.[49] On November 6, 2018, **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]** emailed additional questions asking

---

[46] *See* Recommendation Exhibit 91 at EB-1981-82.

[47] Recommendation Exhibit 32 at EB-576.

[48] *See* Recommendation Exhibit 32 at EB-577. To CTA's knowledge, there had been no such inspections.

[49] *See* Recommendation Exhibit 92 at EB-1984.

CTA to "provide information management policies governing the sharing of U.S. customer information between [CTA] and its ultimate parent company, China Telecom Corporation. For example, how is personally identifiable information from U.S. customers treated and/or accessed?"[50] Team Telecom also requested a description of "the various business roles and responsibilities" among CTA and its affiliated companies.[51]

CTA responded to these questions on December 6, 2018,[52] and provided Team Telecom CTA's information security policy and its U.S. Records Security Agreement with CTCL.[53]

At this point a new Team Telecom representative, **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]** of the National Security Division, replaced **[BEGIN CONFIDENTIAL]** [redacted]. [redacted] **[END CONFIDENTIAL]** did not join National Security Division until November 2018,[54] so she may have limited knowledge of the prior 11 years of Team Telecom meetings and correspondence with CTA. In her letter of March 21, 2019, **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]** sought to reconfirm compliance with the access to records provisions of the 2007 LOA. **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]** also raised new questions about the sharing of U.S. Records with CTA's affiliates,[55] as had been described by CTA in the U.S. Records Security Agreement provided in

---

50 *See* Recommendation Exhibit 35 at EB-587.

51 *See id.*

52 *See* Recommendation Exhibit 36 at EB-589.

53 *See* Recommendation Exhibit 36 at EB-590-654.

54 **[BEGIN CONFIDENTIAL]** [redacted]. **[END CONFIDENTIAL]**

55 *See* Recommendation Exhibit 96 at EB-2002.

December 2018, and as previously discussed in CTA's 2016 letter to Team Telecom.[56] On April 4, 2019, CTA again confirmed what it had repeatedly confirmed before, namely that U.S. Records remained available for inspection in California, that it had not provided any such records to any foreign government pursuant to legal process, and that its disclosure of U.S. Records to its affiliates did not breach any U.S. law or regulation or any provision of the 2007 LOA.[57]

In response to **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]** questions about CTA-affiliate access to U.S. Records, CTA stated that **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]** and that **[BEGIN CONFIDENTIAL]** [redacted][58] **[END CONFIDENTIAL]** CTA further explained that:[59]

> [p]rior to 2013, all CTA U.S. Records were retained on CTA servers in Herndon, VA in the database platform known as 'BOSS.' Beginning in May 2013, when the **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]** was implemented, U.S. records were available to CTA's non-US affiliates abroad.

CTA stated that copies of its U.S. Records for most services were located on the **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]** but with respect to cellular (*i.e.*, MVNO) records, that "no non-U.S. affiliates have ever had access to U.S. Records on AWS."[60]

---

[56] *See* Recommendation Exhibit 125 at EB-2783.

[57] *See* Recommendation Exhibit 103 at EB-2111.

[58] *Id.*

[59] *Id.*

[60] Recommendation Exhibit 103 at EB-2112. CTA provided additional information regarding the types of information contained on AWS in its April 18, 2019 response to Team Telecom. *See* Recommendation Exhibit 107 at EB-2142-49.

[BEGIN CONFIDENTIAL] [redacted] **[END CONFIDENTIAL]** also asked if CTA provided notice to Team Telecom before making a copy of U.S. Records available in China, even though the LOA contains no such requirement. CTA explained that:

> CTA's LOA does not require notice to be provided prior to making U.S. Records available at non-U.S. locations. As such, CTA has not submitted any notification to the DOJ, FBI or DHS prior to making U.S. Records (or copies) available at any non-U.S. location. As you are aware, CTA and Team Telecom have maintained a continuous dialogue on this issue for at least five years.[61]

2. The Recommendation's Description of CTA's U.S. Records is Misleading.

The Recommendation focuses heavily on the sharing of U.S. Record information held by CTA with its Chinese affiliates,[62] apparently because Team Telecom thinks the content of CTA's U.S. Records reveal information that could be helpful to cyber-attacks on U.S. persons or networks. However, Team Telecom vastly overstates the risks associated with CTA's U.S. Records given the actual content and locations of those records. In reality, the types of information that CTA shares with its non-U.S. affiliates are substantially the same types of information that ***any*** U.S. carrier, regardless of its ownership, likely would have to provide to a Chinese carrier if it wants to deliver international services between the two countries.

CTA collects and maintains only limited customer information as U.S. Records. Consistent with common industry practice, this information is shared with CTA's business partners (including its non-U.S. affiliates and its U.S. vendor partners) for purposes of service installation and provisioning. For example, if a customer orders a private line circuit between its U.S. location and a destination in China, CTA will necessarily obtain the customer's contact and billing information, and the endpoints, routing, and configuration of the circuit in question. Some of this information

---

[61] *Id.*

[62] Recommendation, pp. 17-26, 40, 43, 54-55.

must be shared with the foreign carrier that terminates the circuit in China; without such sharing, it would be impossible to provision the service. However, the information obtained is limited to that necessary to provision and bill for the particular service ordered by the customer.

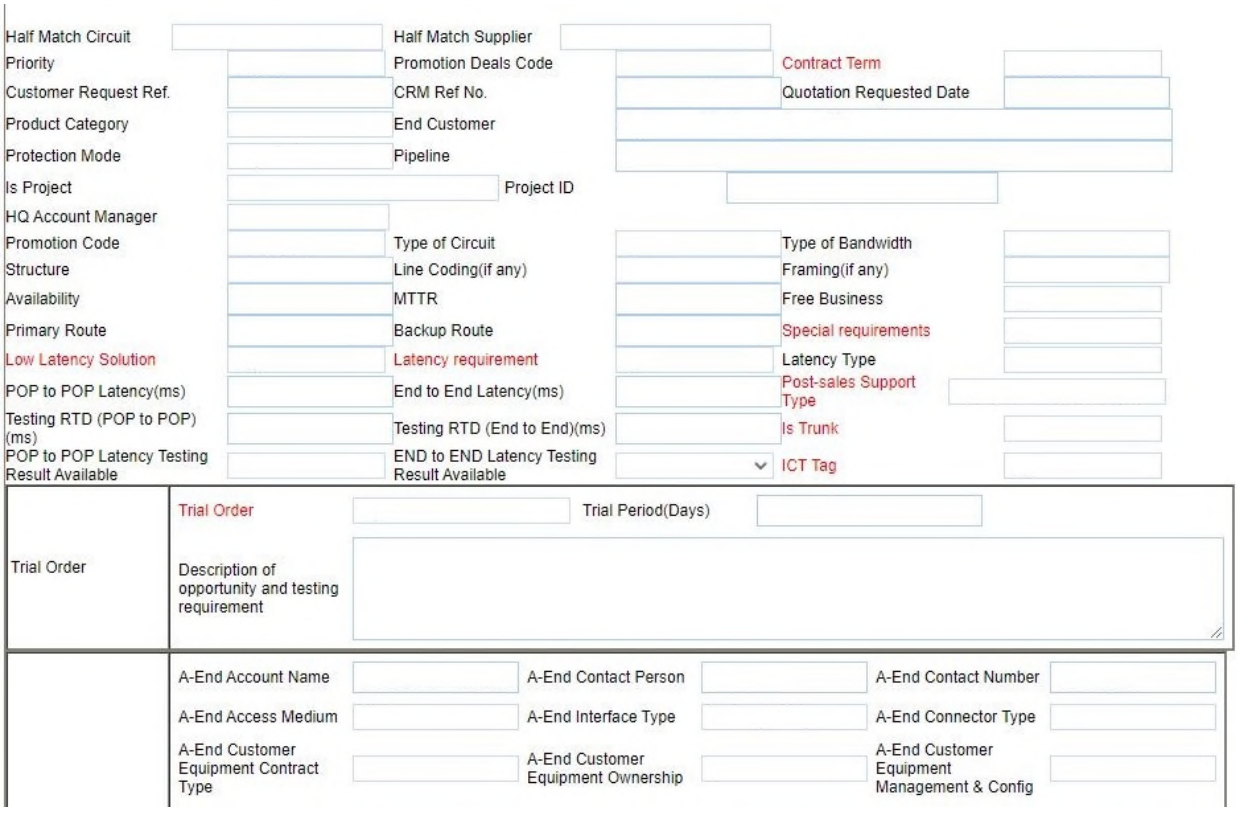
Enterprise and wholesale customers. For international dedicated circuit and enterprise data services, the data collected from U.S. subscribers is plain-vanilla billing information.

A screen shot of typical international data circuit customer data is set out below.

General Info. | Business Info. | Fee Info. | Others Info. | NOC Upate Notice. | Agent Info. | Account Info.

Product		Type		Order Status	
Quote Ref. No.		Order Number		Original Order No.	
Customer Name				Customer Number	
Account Name				Installation Type	
Coordinating Carrier		Account Manager		Billing Manager	
Billing Contact Person		Billing Contact Number		Income Type	
Billing Contact Address					
Create Date		Creater		Sign Date	
RFS Date		Deliver Date		Customer Category	
Billing Start Date		Billing Stop Date		Cross-border business	
Product Instance ID		Service Ref. No.		Circuit ID (CRM)	
CT's Order/Agreememt Template without amendment?		Whether any existing MSS Contract Application No. for the orders		Select MSS Contract	
Signer				Is Agent	
Additional Information					

Historical Cross Region Order					
Related Cross Region Circuit	No.	Singer	Ref No.	Order Ref No.	Circuit No.
	/	/	/	/	/

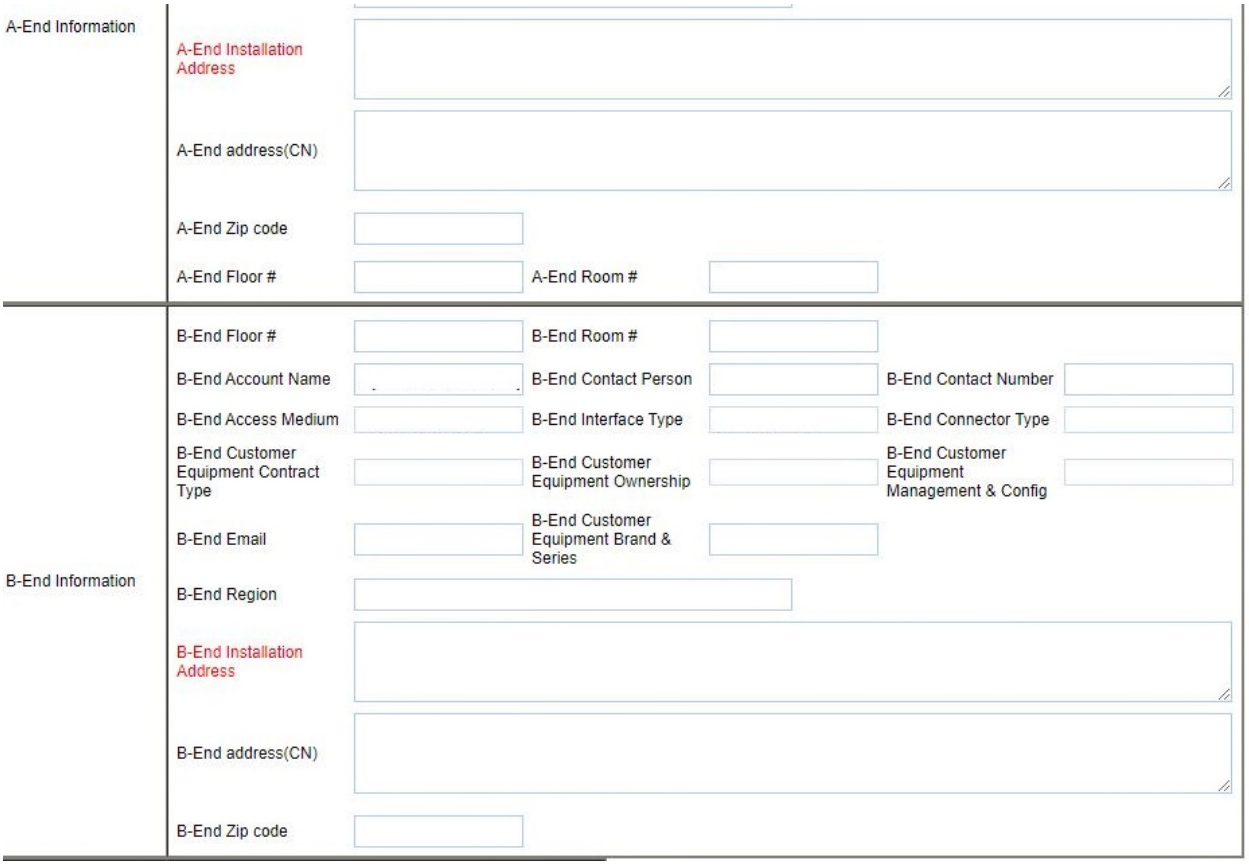


Half Match Circuit		Half Match Supplier			
Priority		Promotion Deals Code		Contract Term	
Customer Request Ref.		CRM Ref No.		Quotation Requested Date	
Product Category		End Customer			
Protection Mode		Pipeline			
Is Project		Project ID			
HQ Account Manager					
Promotion Code		Type of Circuit		Type of Bandwidth	
Structure		Line Coding(if any)		Framing(if any)	
Availability		MTTR		Free Business	
Primary Route		Backup Route		Special requirements	
Low Latency Solution		Latency requirement		Latency Type	
POP to POP Latency(ms)		End to End Latency(ms)		Post-sales Support Type	
Testing RTD (POP to POP) (ms)		Testing RTD (End to End)(ms)		Is Trunk	
POP to POP Latency Testing Result Available		END to END Latency Testing Result Available		ICT Tag	

Trial Order	Trial Order		Trial Period(Days)		
	Description of opportunity and testing requirement				

	A-End Account Name		A-End Contact Person		A-End Contact Number	
	A-End Access Medium		A-End Interface Type		A-End Connector Type	
	A-End Customer Equipment Contract Type		A-End Customer Equipment Ownership		A-End Customer Equipment Management & Config	

A-End Information	A-End Account Name		A-End Contact Person		A-End Contact Number	
	A-End Access Medium		A-End Interface Type		A-End Connector Type	
	A-End Customer Equipment Contract Type		A-End Customer Equipment Ownership		A-End Customer Equipment Management & Config	
	A-End Email		A-End Customer Equipment Brand & Series			
	A-End Region					
	A-End Installation Address					
	A-End address(CN)					
	A-End Zip code					
	A-End Floor #		A-End Room #			
B-End Information	B-End Floor #		B-End Room #			
	B-End Account Name		B-End Contact Person		B-End Contact Number	
	B-End Access Medium		B-End Interface Type		B-End Connector Type	
	B-End Customer Equipment Contract Type		B-End Customer Equipment Ownership		B-End Customer Equipment Management & Config	
	B-End Email		B-End Customer Equipment Brand & Series			
	B-End Region					



As shown above, for international dedicated circuit and enterprise data services, CTA collects basic customer information related to the services ordered, including billing contact and address, location of the service, price of service and type of service. Contrary to the Recommendation,[63] CTA does not collect any other personally identifiable information ("PII") from these customers. The information obtained is limited to that needed to provision and bill for the service ordered. In some cases, such as **[BEGIN HIGHLY CONFIDENTIAL]** [redacted] **[END HIGHLY CONFIDENTIAL]** CTA has agreed to electronic bonding arrangements

[63] *See* Recommendation, pp. 22-24 (alleging significant national security concerns with allowing access "to PII and technical network information, including the potential that such information may be used by foreign governments to target specific individuals and private sector entities").

that give these carriers essentially the same type of U.S. customer information relating to the services they provide as CTA's affiliates in China have with respect to the services *they* provide.

The Recommendation exaggerates the significance of these records and implies that CTA has access to extensive technical data about the U.S. communications and information services used by its enterprise customers. For example, the Recommendation states "China Telecom may have allowed its Chinese affiliates to access U.S. records in China, including enterprise customers' '[t]echnology used and technical configuration; Location of connections and destinations … Vendor and Supplier Information.'"[64] However, the category "technology used and technical configuration" does not mean the technology used *by* customers or information about the configuration of their U.S. or global information technology networks; rather, it refers to the technology that CTA uses or purchases from other carriers to serve these customers. Similarly, "location of connections and destination" refers to the destinations and connections of the circuits that CTA provides to these customers; and "vendor and supplier information" is information about the underlying carrier that provides services or circuits that CTA uses to serve these customers; not information about every vendor and supplier that a customer has relationships with.

MVNO customers. U.S. Records created in connection with CTA's cellular (*i.e.*, MVNO) customers are maintained very differently and no part of those records are available to CTA's Chinese affiliates except when a customer wants to link a Chinese telephone number to their U.S. account.

CTA acts as an MVNO in the U.S. under the "CTExcel" brand name, which CTA markets primarily to Chinese language users in the United States. CTA resells service over the T-Mobile network through an arrangement with **[BEGIN HIGHLY CONFIDENTIAL]** [redacted]

[64] Recommendation, p. 43.

[redacted]. [redacted] **[END HIGHLY CONFIDENTIAL]** interconnects to **[BEGIN HIGHLY CONFIDENTIAL]** [redacted] **[END HIGHLY CONFIDENTIAL]** to provision mobile services on **[BEGIN HIGHLY CONFIDENTIAL]** [redacted] **[END HIGHLY CONFIDENTIAL]** for a CTA customer. CTA collects basic billing information from subscribers, such as name, address, phone type, and credit card information, since consumers pay via credit card. CTA then provides to **[BEGIN HIGHLY CONFIDENTIAL]** [redacted] **[END HIGHLY CONFIDENTIAL]** the information it needs to establish service. CTA's copy of the information provided to **[BEGIN HIGHLY CONFIDENTIAL]** [redacted] **[END HIGHLY CONFIDENTIAL]** is held in the cloud on Amazon Web Services. **[BEGIN HIGHLY CONFIDENTIAL]** [redacted] **[END HIGHLY CONFIDENTIAL]** provides call detail records to CTA for billing process and support, all of which are also maintained by CTA on Amazon Web Services. CTA's non-U.S. affiliates have no access to this information.

When a customer purchases both U.S. and China phone numbers linked to a single SIM card,[65] Chinese government regulations require that CTA's Chinese affiliate (not CTA itself) obtain PII about the user to comply with Chinese law to provide mobile service in China. If a user requests a dual phone number, they must supply the following to that affiliate directly:

- Legal name;
- Chinese Photo ID with the expiration date and the issue place, a foreign passport with a valid visa to China, or a "China Pass" document issued to residents of Hong Kong, Macau & Taiwan;
- A photo of the applicant holding their own ID;
- A Chinese number bill (if the applicant applies to have their existing Chinese number as the dual number).

[65] https://www.ctexcel.us/createonecardtwonumber.

Any U.S. carrier that wished to offer a dual number service would have to collect the same information and provide it to the Chinese mobile carrier, regardless of whether the U.S. carrier was Chinese-owned. CTA understands that other companies offer services that are similar to CTExcel's dual SIM product, and these companies can be expected to collect exactly the same type of personal identifying information from their users, and provide it to a Chinese carrier. They would not be able to offer a dual SIM service without doing so.

In sum, the Recommendation's description of CTA's business records is presented out of context in a way that creates the impression that these records are much more extensive than they actually are.

3. CTA's Statements to Team Telecom Regarding Storage and Access to U.S. Records Have Always Been Accurate.

FCC Commissioner Michael O'Reilly wrote in 2015 that Team Telecom had a "haphazard process" that "leaves applicants subject to the whim of the individual members of Team Telecom at [any] exact moment in time." He added that Team Telecom has no "transparent and balanced process" and "any decisions resulting fuel the charge that blatant political influences led to a particular outcome."[66] Those concerns echo in this case.

The Recommendation alleges that Team Telecom "discovered" misrepresentations about CTA's U.S. records "while monitoring China Telecom's LOA compliance over the past year …."[67] This focus on "compliance over the past year" completely disregards CTA's history of compliance with the LOA over a 13-year period, and the extensive and numerous interactions between CTA and Team Telecom, in particular over the last five years. *See* Section V.E below.

---

[66] *See* https://www.fcc.gov/news-events/blog/2015/09/18/team-telecom-reviews-need-more-structure (last accessed May 27, 2020).

[67] Recommendation, p. 17.

As shown above, CTA consistently and correctly stated that the U.S. Records remained "available in the United States in response to lawful U.S. process." Before May 2013, the records were always available to U.S. lawful process when they were stored in the BOSS system located in the United States. The records remained available to U.S. lawful process when CTA transitioned in the ordinary course of business from using an antiquated database (*i.e.*, BOSS) **[BEGIN CONFIDENTIAL]** [redacted].[68] **[END CONFIDENTIAL]** And, they remain available to lawful U.S. process following the completion of CTA's transition to using **[BEGIN CONFIDENTIAL]** [redacted].[69] **[END CONFIDENTIAL]** CTA has neither contradicted itself in that regard nor misrepresented the status of its U.S. records to Team Telecom.

The Recommendation also complains that CTA did not provide database access logs to Team Telecom in 2019.[70] It variously states that CTA "claimed it *could not* provide access logs";[71] "was *unable* to provide those access logs";[72] and "*declined* to provide Team Telecom with access logs."[73] It argues that this was a violation of CTA's obligations under the inter-company U.S. Records Security Agreement, not a violation of the LOA or of any commitment made to Team

---

[68] In its January 2016 letter to Team Telecom, CTA explained that it previously informed Team Telecom in 2014 that "at times between May 2013 and June 2014, U.S. Records were temporarily stored outside of the U.S. during the transition to the **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]** CTA explained that "[d]uring this entire period, CTA had access to these records and the data was available in the U.S. for response to U.S. process." *See* Recommendation Exhibit 125 at EB-2783.

[69] CTA further explained that "[s]ince June 2014, US Records have been stored in the U.S. in the Company's data center in … California." Recommendation Exhibit 125 at EB-2783. CTA also explained that "U.S. Records concerning the Company's mobile services (MVNO) customers are stored in the Amazon Cloud." *Id.*

[70] Recommendation, p. 20.

[71] Recommendation, p. 25 (emphasis added).

[72] Recommendation, p. 28 (emphasis added).

[73] Recommendation, p. 40 (emphasis added).

Telecom.[74] Apart from not alleging any misconduct that is cognizable by the Commission, the Recommendation's version of events does not match up with the facts. Team Telecom asked CTA on March 21, 2019, to "provide all access logs kept by China Telecom Americas regarding non-U.S. affiliate access to U.S. records …. If access logs are not available or difficult to obtain, please explain."[75] CTA responded on April 4 that "[A]ccessing these logs would require significant man-power and time, as it involves machine-level information located on multiple servers."[76] CTA's response did not "decline" to obtain the access logs maintained by its affiliates, or state that it "could not" provide them.

The Recommendation further argues that, by supposedly not disclosing that CTA's affiliates could see its U.S. Records, CTA violated a representation made while negotiating the LOA to "inform Team Telecom if it intends to store any U.S. business records outside the United States prior to doing so."[77] Again, the Recommendation confuses *storage* of records with *access* to those records. CTA did not commit to notify Team Telecom whenever someone outside the United States had access to its records; its sole obligation under the LOA was to give such notice if *a foreign government served legal process on CTA* – which has never happened. The Recommendation describes a "contradiction" that never existed.

---

[74] The Records Security Agreement was implemented voluntarily by CTA in an effort to assure continued compliance with the LOA, but was not required by the LOA. Even if CTA did not implement this private, inter-company agreement strictly according to its terms, this would not demonstrate any violation of an LOA commitment or of any Commission rule, much less sufficient ground on which to revoke a carrier's authorization.

[75] Recommendation Exhibit 96 at EB-2003.

[76] Recommendation Exhibit 103 at EB-2113.

[77] Recommendation at 21, citing Recommendation Exhibit 3 at EB-15.

B. CTA's Statements To Team Telecom Regarding Its Cybersecurity Policies Were Accurate and Timely.

The Recommendation asserts that CTA "delayed six months" in responding to Team Telecom's request for CTA's cybersecurity policies and that this delay "calls into question its willingness to cooperate with Team Telecom to monitor compliance with the LOA."[78] It argues that CTA is untrustworthy because it "did not immediately disclose that it lacked a formal cybersecurity policy at the time."[79] Of course, the LOA does not require a formal cybersecurity policy. All it requires is that CTA "take all practicable measures" to effectively prevent data breaches from occurring, *not* that it maintain a single, comprehensive written cybersecurity policy. In short, the Recommendation is claiming that CTA "did not immediately disclose" something that it was never asked for and had no obligation to have or to disclose.

The Recommendation also asserts that the absence of a single, formal cybersecurity policy made CTA's statements to customers that it provided a "secure" service false and misleading. That is incorrect as a matter of fact and law. Significantly, the Recommendation never even suggests that CTA's services were not in fact secure. The Information Security Policy submitted to Team Telecom on December 6, 2018, was *not* CTA's first formal cybersecurity policy — it was an effort to comprehensively memorialize numerous cybersecurity and privacy policies already implemented by CTA.

1. CTA's Response was Timely.

Team Telecom's June 2018 request, in addition to seeking "copies of China Telecom Americas' cybersecurity policies and procedures," sought answers from CTA to seven additional

---

78 Recommendation, p. 17.

79 *Id.*

questions regarding its cybersecurity efforts, vendor selection, and requests by the Chinese government to inspect or obtain information about CTA's operations.[80] Following receipt of Team Telecom's request, counsel for CTA corresponded with Team Telecom twice via e-mail regarding the status of CTA's response.[81] Then, on October 1, 2018, CTA provided initial substantive responses to Team Telecom's questions.[82] Team Telecom did not respond to CTA's October 1, 2018 submission for over a month and then requested copies of policies and additional information about "information management policies governing the sharing of U.S. customer information" between CTA and its ultimate parent, and a description of "the various business roles and responsibilities that are within the scope of CTA and those roles and responsibilities that reside with CTG and/or Chin[a] Telecom Corporation."[83] CTA's counsel acknowledged receipt of the request, and Team Telecom responded with thanks the next day.[84]

It was not until November 15, 2018, that Team Telecom set a December 7 deadline for CTA's responses.[85] This was the first and only deadline that Team Telecom provided in connection with its June 2018 request for information. Counsel for CTA responded to Team Telecom nearly immediately and indicated that counsel expected "to get to you the company's U.S. Records Security Agreement shortly."[86] But before that could be done, Team Telecom sent a further request

---

[80] Recommendation Exhibit 32 at EB-576.

[81] *See* Recommendation Exhibit 33 at EB-578-79 (counsel's acknowledgement of receipt of the June 13, 2018 request and August 30, 2018 response to Team Telecom's request for a status update).

[82] *See* Recommendation Exhibit 92 at EB-1983-85.

[83] *See id.*

[84] *See* Recommendation Exhibit 35 at EB-586.

[85] *See* Recommendation Exhibit 35 at EB-586.

[86] *See* Recommendation Exhibit 35 at EB-585.

seeking an explanation of CTA's CALEA compliance policy and a "list [of] other companies that are used by CTA and CTExcel to fulfil (sic) all government legal service."[87] Following these numerous requests and correspondence between Team Telecom and counsel for CTA, CTA submitted its Information Security Policy and responses to Team Telecom's additional questions on December 6, 2018.[88] When Team Telecom had follow up questions about the December 6 submission, CTA, through counsel, responded to those questions.[89]

Throughout this half-year period, Team Telecom never expressed any concern with the timeliness or completeness of CTA's response to its questions, which continued to grow between its June request and the final exchanges of information in January 2019. Yet the Recommendation frames this ongoing exchange of communications as an unreasonable delay that makes CTA untrustworthy for purposes of monitoring compliance with its LOA. Had Team Telecom desired CTA to respond to its request by a date certain, it could have done so in its initial request in June 2018, or in any of its subsequent correspondence over the next five months. It did not. The Recommendation now seeks to fault CTA for missing a deadline that Team Telecom never conveyed.

---

87 *Id.*

88 *See* Recommendation Exhibit 36 at EB-589-654.

89 *See* Recommendation Exhibit 37 at EB-655-57.

As a general matter, CTA has diligently responded to Team Telecom. It has repeatedly confirmed its compliance with the LOA in writing upon Team Telecom's request,[90] provided required notices under the LOA (*e.g.*, regarding a change in designated point of contact),[91] and answered questionnaires and other inquiries from Team Telecom on at least five occasions.[92] Just since retaining current counsel in 2016, CTA has exchanged correspondence and participated in teleconferences and meetings with Team Telecom through counsel on at least 90 occasions. The Recommendation presents an inaccurate picture of CTA's cooperation with Team Telecom, and ignores CTA's consistently timely responses to all of Team Telecom's requests and questions.

2. CTA Did Not Make Inaccurate Statements to its Customers.

Assertions that CTA "may have" made inaccurate statements to U.S. customers about its cybersecurity practices[93] and "may have" failed to comply with U.S. cybersecurity and privacy laws[94] are pure speculation. More fundamentally, such allegations do not articulate any specific claims of violating rules or regulations under federal or state law; and, as noted, there is no evidence that CTA's services were not in fact secure. These arguments should be given no weight by the Commission.

The Recommendation cites no legal requirement or precedent that renders an alleged lack of a single written cybersecurity policy as tantamount to a lack of data security. The cited Federal

---

[90] *See, e.g.*, Recommendation Exhibit 91 at EB-1979-82.

[91] *See, e.g.*, Recommendation Exhibit 125 at EB-2781-83.

[92] *See, e.g.*, Recommendation Exhibit 92 at EB-1983-85; *See* Recommendation Exhibit 36 at EB-589-654; Recommendation Exhibit 78 at EB-1888-1893; Recommendation Exhibit 37 at EB-655-57; and Recommendation Exhibit 103 at EB-2107-2114.

[93] Recommendation, p. 26.

[94] Recommendation, pp. 26, 28.

Trade Commission ("FTC") case against AshleyMadison.com (a dating site) proves that point. AshleyMadison.com suffered a massive data breach,[95] which the FTC attributed to AshleyMadison.com's failure to engage in "a number of practices that, taken together, failed to provide reasonable security."[96] The FTC based its claim on "practices," not documentation. Here, there is no claim either that CTA failed to take reasonable security measures, or that anyone was injured by any such failure. The FTC never articulated the notion that the mere lack of a written policy either violated federal law or even was related to the AshleyMadison.com security failures. Indeed, the Director of the FTC's Bureau of Consumer Protection admitted that the FTC is "mindful" that its data security orders have been "struck down" by at least one federal appeals court as "unenforceably vague."[97] The suggestion that CTA has violated "federal law" merely because it did not compile a single written policy document before 2018 simply lacks foundation.

The Recommendation's claim that CTA's "lack of a formal cybersecurity policy prior to December 2018 may potentially run afoul of federal law" relies on the premise that CTA made misrepresentations to customers regarding its services' security.[98] But, the Recommendation does not identify any specific statements that the Executive Branch contends were inaccurate except citing to out-of-context quotes from CTA's website using broad terms like "maximum security"

---

[95] *See FTC v. Ruby Corp*, https://www.ftc.gov/system/files/documents/cases/161214ashleymadisoncmplt1.pdf (last accessed May 21, 2020).

[96] For example, the FTC alleged failures to implement reasonable access controls, to conduct adequate training, and to ascertain third-party service provider security capabilities.

[97] A. Smith, Director, FTC Bureau of Consumer Protection, Blog Post (January 6, 2020), https://www.ftc.gov/news-events/blogs/business-blog/2020/01/new-improved-ftc-data-security-orders-better-guidance (last accessed May 21, 2020).

[98] Recommendation, p. 28.

and "mission-critical data."[99] It does not offer any evidence that even remotely suggests CTA offered something less,

It also argues that CTA "targeted" U.S. customers in certain industries (*e.g.*, financial, logistics, retail, energy, media and healthcare).[100] First, this is a *non sequitur* – whether CTA did or did not misrepresent its level of security depends on *what* it said, not on *who* it was speaking to. Second, CTA does not seek out customers in particular industries; rather, CTA seeks out customers in any industry who have a particular need for communications with China. As Exhibit 8 details, CTA serves customers in a wide range of industries, whose common denominator is a business interest in China. The unspoken but clear implication that CTA somehow "targeted" customers based on some factors other than commercial interests is unsupported by any evidence, and inconsistent with CTA's actual customer profile.

The Recommendation also fails to present any valid reason for suggesting "questions about whether [CTA] complied with [certain] state laws[.]"[101] As discussed below, CTA developed and complied with numerous security policies, including policies that were written and implemented before December 2018. And, just like the LOA, no state or federal law mandates that businesses have a *single* overarching policy. Rather, they require at most that businesses "implement and maintain reasonable" security procedures. For example, while the Ohio law references a "written" cybersecurity program, it does so in the context of a "voluntar[y]" action by companies who wish to assert an affirmative defense against claims relating to a data breach.[102] The Recommendation's

---

99 *Id.*

100 *Id.*

101 Recommendation, pp. 30-31.

102 Ohio Rev. Code Ann. §1354.02(D) (West, 2018).

citation to the California privacy policy law is even more inapposite. That statute provides that "[a]n operator shall be in violation of this subdivision only if the operator fails to post its policy within 30 days after being notified of noncompliance."[103] CTA received no such notification of non-compliance and therefore, by the letter of the California law, cannot be considered in violation.

The Recommendation's assertion that CTA "may have" violated these laws and/or regulations is pure speculation without any factual or legal basis.

V. The Commission Should Reject Allegations That CTA's Services Are Not in the Public Interest Because It Is Owned by Chinese Parent Entities.

It is clear from the overall tone and content of the Recommendation that its efforts to claim misconduct by CTA – which, as shown in Section IV above, are based on misleading and inaccurate narratives – are mostly for window-dressing. The principal thrust of the Recommendation is that CTA's offering of telecommunications services in the United States is not in the public interest solely because CTA is owned by a publicly-traded Chinese company, which in turn is indirectly controlled by the government of the People's Republic of China.[104] The Recommendation essentially argues that any carrier that is indirectly owned by the Chinese government would be "vulnerable to exploitation, influence and control by the Chinese government."[105]

As stated in Section II above, the Commission should not revoke a carrier's existing Section 214 authorization based on such policy concerns, but only upon evidence (which is not offered in the Recommendation) of a violation of law or regulation by the licensed carrier. And apart from

---

[103] Cal. Bus. & Prof. Code § 22575(a) (West, 2018).

[104] *See* Exhibit 1 for a description of the ownership and control of CTA; and Exhibit 3 for a description of CTA's corporate governance.

[105] Recommendation, p. 34.

that legal consideration, the Recommendation exaggerates and misstates the facts on which its claims are based, and therefore should be rejected by the Commission.

Apart from factual errors in the Recommendation's analysis, which are discussed in the following sections, the Team Telecom factors rely heavily on subjective judgments as to the so-called "trustworthiness" of CTA. CTA can and does respond to the factual allegations that Team Telecom claims support its evaluation of trustworthiness, but CTA is not in any position to express an opinion about the Executive Branch's position on alleged policies of the Chinese government, nor is it able to respond to Team Telecom's subjective evaluation of these factors. The Commission should not revoke an individual carrier's section 214 authorizations based solely on foreign policy concerns in the absence of any evidence whatsoever of specific misconduct by the carrier in question.[106]

CTA is responding to the Recommendation as an independent, profit-seeking business based in the United States, operating in the United States, serving many U.S. customers, and employing many U.S. citizens and permanent residents among its employees. Any implication that CTA's employees would be disloyal to the United States because they work for a Chinese-owned company is offensive and insulting.

[106] *See* Section II, above.

A. CTA is Not Subject to the Exploitation, Influence, or Control of the Chinese Government.

The Recommendation claims to identify a series of factors, starting with CTA's corporate ownership, that all point back to China and the alleged vulnerability of CTA to "exploitation, influence, or control" by the Chinese government.[107] CTA incorporates Exhibit 15 herein by reference, in which it responds to these claims of "exploitation, influence, or control." Essentially, the Recommendation asks the Commission to disregard CTA's existence as a separate corporate entity.

CTA has held section 214 authorizations since 2002, and has been party to an LOA with Team Telecom since 2007. For nearly two decades, CTA has worked to comply with U.S. law and Commission regulations. There is no evidence that, in nearly two decades of operation, CTA has ever attempted to do anything contrary to the interests of the United States. And, as discussed in Section V.E below, the allegations in the Recommendation relating to the LOA are unfounded. There is no reasonable basis for the Commission to ignore CTA's track record of regulatory compliance and lawful operation in the public interest.

CTA is a corporation organized and under the laws of the State of Delaware, with its principal place of business in Herndon, Virginia. It also has offices in five other U.S. cities. It has no offices in China. It employs 224 persons in the United States, of whom more than half are either U.S. citizens or permanent residents.[108]

As a corporation governed by the General Corporation Law of the State of Delaware, CTA's directors and management must discharge their fiduciary duties towards CTCL, the sole

[107] *See* Recommendation, pp. 32-52.

[108] *See* Exhibit 3 for a full description of CTA's corporate governance.

shareholder of CTA, in a way that maximizes shareholder return on investment.[109] The directors and officers are fiduciaries, and have duties of care and loyalty to the corporation.[110] A corporate director, however, does not have a duty to follow an illegal instruction from the stockholders; nor does an officer have a duty to follow an illegal instruction from the directors. In fact, their duties are to disobey any such instruction, because "a fiduciary may not choose to manage an entity in an illegal fashion, even if the fiduciary believes that the illegal activity will result in profits for the entity."[111] The Delaware Supreme Court has specifically held that a breach of the duty of loyalty to a corporation occurs where "the fiduciary acts with the intent to violate applicable positive law."[112] In short, the duty of CTA's directors and management to serve its shareholder's (*i.e.*, CTCL) interest in maximizing return does not conflict with the public interest; instead, it is the cornerstone of modern economics for market participants to pursue their own interest while fulfilling public interest.

---

[109] 8 Del. C. § 141(a) ("The business and affairs of every corporation organized under this chapter shall be managed by or under the direction of a board of directors … ."); *McMullin v. Beran*, 765 A.2d 910, 916 (Del. 2000) ("One of the fundamental principles of the Delaware General Corporation Law statute is that the business affairs of a corporation are managed by or under the direction of its board of directors.").

[110] *In re Orchard Enterprises, Inc. Stockholder Litig.*, 88 A.3d 1, 32 (Del. Ch. 2014) (holding that "[d]irectors of a Delaware corporation owe two fiduciary duties—care and loyalty"); *Ivanhoe Partners v. Newmont Mining Corp.*, 535 A.2d 1334, 1345 (Del. 1987) (stating that directors have an "affirmative duty to protect the interests of the corporation…"); *Gantler v. Stephens*, 965 A.2d 695, 708–09 (Del. 2009) (stating that officers have the same fiduciary duties as directors).

[111] Metro Commc'n Corp. BVI v. Advanced Mobilecomm Techs. Inc., 854 A.2d 121, 163–64 (Del. Ch. 2004).

[112] *Stone v. Ritter*, 911 A.2d 362, 369 (Del. 2006) (internal citation omitted).

As detailed in Exhibit 15, CTA is a subsidiary of CTCL, which is a publicly-traded company whose officers and directors likewise owe fiduciary duties to their stockholders, including the minority investors such as Citigroup, BlackRock, and J.P. Morgan Chase.

CTA is subject to the jurisdiction of U.S. courts. It has been served with subpoenas and other legal process on multiple occasions since it received its section 214 authorizations. CTA has responded to more than 20 requests from U.S. law enforcement agencies since at least 2015. It has never invoked "procedural and substantive bars" to service of process.[113] As a Delaware corporation, CTA is required to and does appoint a registered agent for service of process, both in Delaware[114] and in any state in which it is qualified to do business as a foreign corporation, and is fully subject to the process of State and Federal courts in all cases within their respective jurisdictions.

CTA's local management operates independently as a profit-seeking commercial enterprise. Executives of CTA undergo a very thorough interview process and are appointed by its shareholder, not by any foreign government or Party organization. CTA's articles of incorporation and by-laws contain no references whatsoever to any foreign government, any of its agencies, or any foreign political party. CTA management is committed to complying with U.S. law and its responsibilities as a U.S.-regulated common carrier, including compliance with its LOA obligations to Team Telecom.

CTA funds its business operation through revenues generated from customers in arm's length commercial transactions. It does not receive any grants, subsidies, or loans from any foreign

---

[113] *China Mobile*, 34 FCC Rcd at 3368-69, ¶ 16 (discussing "the difficulties of serving process in the United States in order to enforce U.S. law on Chinese companies … operating within the United States").

[114] *See* Delaware Secretary of State, General Information Name Search, https://icis.corp.delaware.gov/Ecorp/EntitySearch/NameSearch.aspx.

government. It pays U.S. taxes on its U.S. revenue, income, and property. When CTA enters into transactions with its foreign affiliates, it negotiates pricing on an arms-length basis. CTA does not receive any preferential pricing from its affiliates.

CTA maintains its own human resources staff, separate from the staff of its parent and affiliated companies, which is responsible for hiring of U.S.-based employees. Of the 224 current employees, 219 were hired by local CTA management; only five were assigned on rotation by the parent company, CTCL. The human resources department maintains internal hiring processes and procedures under which recruiting and hiring are entirely under the supervision of the U.S.-based management of CTA, without interference by or consultation with its parent company and affiliates, except for a handful of the most senior management positions. These processes apply to both the hiring of new employees and decisions on internal transfers and promotions of current employees.

CTA employees (except for the President) are evaluated annually by their U.S.-based managers according to CTA's internal performance policy. Neither CTCL nor any affiliated company plays any role in employee performance evaluations. CTA assesses each employee's performance based solely on their ability to do their job by a standard Company process and key performance indicators ("KPIs"). Employees and their supervisors create three to five annual KPIs based on Company, departmental, and employee development needs. Sales and support teams have established KPIs related to sales targets. The individual KPIs account for **[BEGIN HIGHLY CONFIDENTIAL]** [redacted] **[END HIGHLY CONFIDENTIAL] [BEGIN CONFIDENTIAL]** [redacted]. **[END CONFIDENTIAL]** CTA has a standard KPI **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL] [BEGIN HIGHLY CONFIDENTIAL]** [redacted] **[END HIGHLY CONFIDENTIAL] [BEGIN CONFIDENTIAL]** [redacted]

[redacted] **[END CONFIDENTIAL]**which rates the employee's communication, attitude, team collaboration, quality of work, analysis and problem solving, meeting goals and deadlines, productivity, and attendance. Promotions are recommended and decided by prior performance grades and ratings.

CTA's overall performance, as well, is evaluated by its parent company based on quantitative KPIs that measure its economic and managerial performance (including revenues and revenue growth, collection of accounts receivable, customer retention and growth, cost controls, risk management, and accuracy of financial records). CTA's senior managers' annual bonuses are determined based on the results of this performance evaluation. None of the performance indicators require CTA to carry out any illegal activities or to engage in any actions contrary to the interests of the United States.

All CTA staff undergo constant training on compliance with U.S. laws and regulatory obligations. CTA employees are all aware of their duty to preserve the confidentiality of customer information. Further, as explained in more detail in Section IV.A.2 above, the customer information that CTA does maintain is very limited (and never includes any access to the content of customer transmissions or information stored on a customer's private equipment).

B. CTA is Not Required to Comply with Chinese Government Requests.

It is not the case, as the Recommendation alleges, that "[CTA] will be forced to comply with Chinese government requests without sufficient legal procedures subject to independent judicial oversight[.]"[115] As with many other allegations in the Recommendation, this is based on fear of some future hypothetical event and not substantiated by any proof of existing conduct.

[115] Recommendation, p. 37.

The only example provided in support of this allegation is Team Telecom's bold statement that CTA "has already submitted to at least one foreign request from its Parent Entity without sufficient legal process or judicial oversight." This allegation is both untrue and based on interpretation of a document taken out of context.[116]

First, this allegation appears in a section of the Recommendation that supposedly is evaluating CTA's vulnerability to "*foreign government*" requests, but it does not involve any government request at all. Rather, it describes an internal business decision to implement an internal management platform for global operations, and the electronic versions of CTA's customer records needed to be shared with its non-U.S. affiliates in order for the process to work.[117] Second, CTA entered into an arms-length Records Security Agreement with its parent company expressly for, among other things, the purpose of ensuring compliance with the LOA.[118] So the Recommendation seems to suggest the irrational inference that by entering into a commercial agreement, CTA demonstrated its vulnerability to be directed by and comply with Chinese Government requests.

The Recommendation takes its allegation even further by arguing that the Records Security Agreement does not provide sufficient judicial oversight of access to CTA's records, because any disputes under this agreement are subject to mandatory arbitration to take place in China.[119] This

---

[116] Recommendation, p. 37.

[117] As explained in more detail in Section IV.A above, CTA has always shared information with affiliates in the ordinary course of business to allow provisioning of services that terminate in other countries. In the company's early years, this information was sent to CTA's affiliates by email or fax; the only thing that changed after 2014 was that the information was transmitted electronically.

[118] Recommendation Exhibit 36 at EB-621 (identifying "maintaining compliance with the terms of the CTA Authorizations and the Team Telecom Obligations" as a purpose of the agreement), EB-625-26 (paragraph 2.5.3, incorporating the same restrictions on access to U.S. records as appear in the LOA).

[119] Recommendation, p. 38.

is (once again) a commercial agreement between two commercial entities. Arbitration is a widely used alternative dispute resolution ("ADR") mechanism both in China and worldwide. It is an international standard practice for the international commercial arbitration award to be final and legal binding, without judicial review, unless the arbitration proceeding violated due process or narrowly defined public policy, in which case the affected parties may initiate a proceeding to set aside or invalidate the arbitration awards. These rules and practices are applicable to CIETAC as well as other international arbitration institutions such as American Arbitration Association ("AAA") or ICC.[120] The Chinese courts rarely invalidate international arbitration awards on due process and public policy grounds,[121] and when they do such decisions must be approved by the Supreme People's Court, the highest court of the nation.[122]

---

[120] U.S. public policy strongly favors the enforcement of agreements to arbitrate. *See* 9 U.S.C. § 2 (providing that agreements to arbitrate "shall be valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract"); *Epic Sys. Corp. v. Lewis*, 138 S. Ct. 1612, 1632 (2018) (holding that "the law is clear: Congress has instructed that arbitration agreements … must be enforced as written").

[121] "[N]umerous empirical studies showing Chinese courts rarely reject enforcement of a foreign arbitral award"; "the empirical data suggests that Chinese courts have a high rate of enforcement of foreign arbitral awards, and this rate has increased over time"; "Based on publicly available information, fewer than half of those lower court requests for non-enforcement were approved by the SPC"; "the reported experience of our survey respondents does not show China is dramatically more challenging or difficult than other jurisdictions." *See* UCLA Pacific Basin Law Journal (2016), *Perceptions and Reality: The Enforcement of Foreign Arbitral Awards in China*, https://escholarship.org/content/qt6s1632q5/qt6s1632q5.pdf?t=oee06g; "Chinese courts rarely support requests made by the parties on the grounds of public policy." *See* China Justice Observer (September 15, 2019), *Judicial Review of Arbitral Awards in China: How Courts Apply Public Policy?*, https://www.chinajusticeobserver.com/a/judicial-review-of-arbitral-awards-in-china-how-courts-apply-public-policy.

[122] *See* Article 2 of the Notice of the Supreme People's Court on Issues in the People's Courts' Handling of Foreign-related Arbitrations and Foreign Arbitrations (effective as of August 28, 1995). *See* Article 2 of the Provisions of the Supreme People's Court on Issues relating to the Reporting and Review of Cases Involving Judicial Review of Arbitration (effective as of January 1, 2018).

CIETAC's arbitration rules are modeled after and substantially the same as the ICC rules and the UNCITRAL model rules.[123] Parties to CIETAC arbitrations are free to choose their own arbitrators, and the arbitration proceedings and final awards are non-public to protect the confidentiality of the parties unless the parties both chose to make them public. CIETAC is one of the world's largest and busiest arbitration institutions based on case-load. According to public data, in 2019 alone, CIETAC received over 3,000 arbitration applications in total, in which 617 applications involve foreign parties from 72 countries.[124] The total amount in dispute is more than US$17.5 billion, of which US$5.4 billion is foreign related.[125] CIETAC arbitration awards have been widely recognized and enforced internationally, including in the United States.[126] During its

[123] CIETAC, "Arbitration Rules," http://www.cietac.org/index.php?m=Page&a=index&id=106&l=en.

[124] *See* CIETAC 2019 Work Report (section I 2019 Work Summary) in English, http://www.cietac.org.cn/index.php?m=Article&a=show&id=16871&l=en .

[125] *Id.*

[126] "In its past 60 years, CIETAC has resolved over 30,000 international and domestic disputes, earning a reputation of impartiality and efficiency; as a result, CIETAC awards have been recognized and enforced by such foreign jurisdictions as the United States, United Kingdom, Germany, Japan and Canada." *See* Vancouver Economic Commission, *Chinese International Economic and Trade Arbitration Commission (CIETAC) Announces New North American HQ in Vancouver*, https://www.vancouvereconomic.com/blog/vecs_take/chinese-international-economic-trade-arbitration-commission-cietac-announces-new-north-american-hq-vancouver/; for enforcement in the United States, s*ee* Kluwer Arbitration Blog, *CIETAC Arbitration Award Enforced in the U.S. Despite Alleged Forgery in the Underlying Agreement* (October 6, 2018), http://arbitrationblog.kluwerarbitration.com/2018/10/06/cietac-arbitration-award-enforced-in-the-u-s-despite-alleged-forgery-in-the-underlying-agreement/; for enforcement in India, see Herbert Smith Freehills, *Delhi High Court Agrees To Enforce CIETAC Arbitral Award Against Indian Company Despite CIETAC Split*, https://www.mondaq.com/india/international-courts-tribunals/727502/delhi-high-court-agrees-to-enforce-cietac-arbitral-award-against-indian-company-despite-cietac-split; for enforcement in England, see Latham & Watkins, *English Court of Appeal Re-Affirms Pro-Enforcement Stance Toward Foreign Arbitral Awards* (May 30, 2018), https://www.latham.london/2018/05/english-court-of-appeal-re-affirms-pro-enforcement-stance-toward-foreign-arbitral-awards/; and for enforcement in Canada, *see* Tianjin v. Xu, 2019 ONSC

more than 60 years' history, CIETAC has earned its international reputation and impact, and has established cooperation with multiple international arbitration institutes worldwide, including the AAA.[127] Thus, CTA has no reason to believe that the provision for CIETAC arbitration would not provide it reasonable protection for its interests under the Records Security Agreement.

Further, the Recommendation argues that due to its ownership, CTA could be forced to provide information to the Chinese government under Chinese laws, including the 2017 Cybersecurity Law and 2018 Regulation on Internet Security Supervision (the "2018 Regulation").[128] Again, the relevant articles from the 2017 Cybersecurity Law and the 2018 Regulation cited by the Executive Branch are taken out of context, to suggest that relevant government authorities in China will have unrestricted powers in requesting information or extensive cooperation from CTA. This not true if these articles are considered together with other relevant articles from the PRC laws and regulations cited by the Executive Branch in the Recommendation.

---

628 (heard on January 16, 2019), https://www.canlii.org/en/on/onsc/doc/2019/2019onsc628/2019onsc628.html.

[127] "Senior AAA officials made a weeklong trip to China that resulted in the signing of a new cooperative agreement with the CIETAC. This agreement, which supplements prior accords, is the first to include concrete initiatives for mutual administrative assistance in setting up arbitration proceedings in either the United States or China. It also provides for cooperation in promoting arbitration as a means of settling international commercial disputes and in running educational conferences and seminars on conflict management." *See* American Arbitration Association, *2001 President's Letter and Financial Statements*, https://www.adr.org/sites/default/files/document_repository/2001%20Annual%20Report_0.pdf; for other international arbitration institutions that entered into cooperative agreement with CIETAC, *see* CIETAC, *CIETAC Signed Cooperation Agreements with Six International Arbitration Institutions in Beijing and Reached Consensus on Further Cooperation*, http://www.cietac.org.cn/index.php?m=Article&a=show&id=16310&l=en.

[128] Recommendation, pp. 38-40. As the Recommendation recognizes, "these new laws codified existing practices rather than imposing wholly new obligations." Recommendation, p. 40. Thus, the adoption of these laws would not seem to have created any new risks or vulnerabilities, even if the Recommendation's analysis of them were correct.

First, article 2 of the Cybersecurity Law states that the law applies to the "construction, operation, maintenance, use of networks, as well as the supervision and management of cybersecurity, within the territory of the [People's Republic of China]." CTA does not engage in any of the aforementioned business in China. The 2017 Cybersecurity Law therefore gives the Chinese government no authority over CTA's operations in the United States. CTA is governed by U.S., not Chinese, laws.

Second, the 2018 Regulation was formulated and promulgated according to the Cybersecurity Law and the Police Law of the People's Republic of China.[129] Those laws, pursuant to which the 2018 Regulation was formulated and promulgated, are applicable only within the territory of China. And the 2018 Regulation applies when the Ministry of Public Security and its local counterparts supervise and conduct inspections about the compliance with applicable PRC cybersecurity laws and regulations by Internet service providers and Internet users.[130] The competent authority for enforcement is the Chinese public security authority, which does not have the ability to enforce law beyond the borders of the People's Republic of China. [131] Therefore, the promulgation of the 2018 Regulation does not render CTA's operations in the United States under supervision or inspection by the Chinese public security authority.

Further, whatever implications the 2017 Cybersecurity Law has for carriers that do operate in China, these would not be affected by revocation of CTA's authorizations. Any U.S. carrier that

---

[129] *See* article 1 of the 2018 Regulation on Internet Security Supervision.

[130] *See* article 2 and article 8 of the 2018 Regulation on Internet Security Supervision.

[131] The implementing authority for the supervision and inspection under the 2018 Regulation "should be the public security organs in the place where the network service operators of the Internet service providers or the network management agencies of the Internet users are located". *See* article 8 of the 2018 Regulation on Internet Security Supervision. Also, if the internet service provider is an individual, the implementing authority should be the public security organ of the habitual residence of the individual. *Id.*

provides services to destinations in China, regardless of its ownership, will have to do so by connecting with a Chinese network that is subject to the provisions of Chinese law. There is no rational link between CTA's U.S. authorizations and the Chinese government's regulation of its parent company's operations in China.

C. Allegations That CTA's U.S. Operations Provide Opportunities for Economic Espionage Against U.S. Targets Are Unfounded.

The Recommendation charges that "[CTA's] U.S. operations provide the Chinese government with access to valuable targets for economic espionage and other intellectual property and privacy-related thefts. The international section 214 authorizations furnish [CTA] with access to more customers, communications traffic, and interconnections with other U.S. common carriers than it would have otherwise."[132] The assertion is not based on any CTA misconduct—indeed, none of the examples that the Recommendation cites even involve CTA. CTA has no knowledge of, and therefore cannot comment on, any of these examples.

Moreover, CTA's business model, including its access to customer data, does not provide what the Recommendation suggests as opportunities for economic espionage. *See* Section III above.

The Recommendation implies that CTA's Managed Service Provider ("MSP") offering could be misused to provide "abundant opportunities" for hacking activities.[133] But CTA's MSP service offers no access to the data on its customers' computers. The term "managed services provider" is extremely vague and encompasses a range of different capabilities, depending on who is using it. Different MSPs offer a range of different capabilities, with differing levels of access to

[132] Recommendation, p. 41.

[133] *Id.*

their clients' equipment. CTA's MSP service—"NetCare"—only monitors connectivity and transmission quality on the CTA-provided circuit, and does not have access to any customer-owned equipment unless the customer authorizes that access for trouble-shooting purposes.

The Recommendation then suggests a scenario that CTA could be co-opted in sending e-mails that "might actually be from network management."[134] This scenario is entirely speculative; CTA does not serve as an outsourced "network management" for any U.S. company, and the Recommendation ignores CTA's long record of compliance with U.S. law. Speculation on what is essentially no more than a threat of phishing emails does not support the drastic remedy of revocation.

The Recommendation also speculates that CTA's Chinese affiliates may misuse records CTA maintains about its U.S. customers.[135] But the records CTA collects and maintains about its customers are those necessary to provision and bill for services, and are substantially similar to the records that *any* U.S. carrier would have to share with Chinese carriers to enable service between U.S. and China. *See* Section IV.A.2 above. The Recommendation's allegation regarding CTA's Chinese affiliates' maintenance of database access logs is similarly flawed. *See* Section IV.A.3 above. Such flawed logic cannot possibly sustain the Commission's burden to show by clear and convincing evidence egregious misconduct by CTA.[136]

---

[134] Recommendation, p. 43.

[135] Recommendation, p. 43.

[136] The Recommendation also mentions two economic espionage cases allegedly conducted by Chinese state-sponsored actors. Recommendation, pp. 4-5. Neither involves CTA or its affiliates, and CTA has no knowledge of either of these cases. The Recommendation provides no basis to believe that CTA's U.S. operations would facilitate these kinds of economic espionage activities.

D. CTA's Operations in the United States Do Not Provide Opportunities to Disrupt and Misroute U.S. Communications Traffic.

The Recommendation asserts that "[CTA's] U.S. operations, particularly its eighteen (18) Points of Presence (PoPs) in the United States, provide Chinese government-sponsored actors with openings to disrupt and misroute U.S. data and communications traffic."[137] It bases this claim on various published reports of supposed "misrouting" incidents that, it says, "are believed to result from Border Gateway Protocol (BGP) announcement errors, in which China Telecom either originated erroneous route information, or propagated and amplified erroneous route information by advertising it to U.S. peering partners."[138] However, it does not provide sufficient technical detail about these allegations to enable CTA or any independent third party to provide a specific response to each one. It is thus fundamentally unfair to expect CTA to defend itself against allegations on this basis alone. But because CTA is expected to provide "a detailed response to the allegations" in the Recommendation,[139] CTA provides an overall response to the general claim in this section that its U.S. operations are somehow involved in misrouting of Internet traffic.[140] They are not.

---

[137] Recommendation, p. 44 (footnote omitted). The Recommendation claims that these facts are relevant to factors 8-10 and 12 of its analysis, which as already noted are inherently subjective and so vague as to encourage arbitrariness. *See* Section II above.

[138] Recommendation, pp. 44-45 (footnote omitted). This section of the Recommendation relies heavily on Demchak, Chris C. and Shavitt, Yuval (2018) "China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking," MILITARY CYBER AFFAIRS: Vol. 3: Iss. 1, Article 7, p. 2, https://scholarcommons.usf.edu/mca/vol3/iss1/7. However, as independent reviewers have pointed out, the article "was unusual in that it didn't provide AS numbers, specific dates and other specifics that allowed other researchers to confirm the claims." Goodin, Dan, Ars Technica, "Strange snafu misroutes domestic US Internet traffic through China Telecom", https://arstechnica.com/information-technology/2018/11/strange-snafu-misroutes-domestic-us-internet-traffic-through-china-telecom/.

[139] See Order to Show Cause, ¶ 12.

[140] As stated in Section I, above, CTA reserves the right to respond to any additional evidence on this subject that may be introduced in any proceeding resulting from the *Order to Show Cause*.

The Recommendation's description of routing issues is fundamentally misleading, and represents either a failure to understand or a misrepresentation of basic principles of Internet architecture and routing.[141] The Internet is not a single network, but rather consists of many thousands of interconnected networks. Each network is called an "Autonomous System" (AS). Most of these independent networks are not connected directly to each other. "A small number of the very large ASs form the 'tier 1' or 'backbone' set of global 'peers' who contract among each other to share massive volumes of traffic reciprocally without paying transit fees. … All other ASs must pay for – or specially negotiate – packet traffic transiting arrangements."[142]

CTCL operates a global network, ChinaNet (AS 4134), which is a Tier 1 network and has many customers operating smaller networks who purchase transit service from it. CTA maintains POPs in the United States that provide access to this network for U.S. transit customers and peering partners. ChinaNet also has interconnections with numerous other transit customers and peering partners, both in China and in third countries.

Border Gateway Protocol ("BGP") is a routing protocol used by ASs to allow routing of traffic between their respective networks. Each AS configures a "routing table" that lists "the IP address blocks that their AS owns, whether to be used as a destination *or as a convenient transit route*."[143] Thus, a Tier 1 AS does not merely list the IP address blocks that it serves directly, but also all the IP address blocks served by any of the networks for which it provides transit service – networks that it does not directly control.

---

[141] In addition, the allegations discussed in this section relate to CTA's Internet traffic exchange services, which are information services and therefore would not be affected by the proposed revocation of the company's section 214 authorizations. *See Restoring Internet Freedom*, 33 FCC Rcd 311, 410 (2018) (classifying internet traffic exchange as an information service).

[142] Demchuk and Shavitt, *supra*, pp. 2-3.

[143] Demchuk and Shavitt, *supra*, p. 3 (emphasis supplied).

BGP was established as a standard relatively early in the development of the global Internet. Like many other early Internet protocols, it depends heavily on trust among participating networks. A Tier 1 network like ChinaNet does not have first-hand knowledge of all the IP address blocks served by its transit customers. Rather, it relies on them to list these address blocks in their own BGP routing tables, and then it propagates this information as part of its own BGP tables. As a result, if a transit customer announces that it serves an IP address block that is not actually on its network, this error can be propagated automatically to higher-level networks and eventually to a Tier 1 network such as ChinaNet. Because BGP routing is based on principles of equality and mutual trust, peering partners generally do not actively monitor, discover and correct errors in real time.

The Recommendation claims that CTA's "failure to monitor its network" is the cause of routing issues.[144] But in reality, internet routing problems are common and occur on all networks despite the best efforts of responsible operators. The BGP protocol is complex and fragile — indeed, the Recommendation itself acknowledges "how inherently fragile BGP is …."[145]

The Internet Society's Mutually Agreed Norms for Routing Security ("MANRS"), a project endorsed in the Recommendation,[146] monitors routing announcements and maintains an "observatory" that records detected incidents. According to the MANRS Observatory,[147] 1,194 "incidents" were detected in April 2020 (an average of about 40 per day), and 967 networks were identified as causing at least one of these incidents. This included 340 incidents originating from

---

[144] Recommendation, p. 49.

[145] Recommendation, p. 50, citing Recommendation Exhibit 101 at EB-2099.

[146] Recommendation, p. 48 & n.177.

[147] *See* MANRS Observatory, Overview, https://observatory.manrs.org/#/overview.

269 U.S.-based networks, and only 24 incidents originating from 18 China-based networks. This is consistent with an analysis of data from 2017 by the Internet Society, which found that the U.S. had the most routing incidents (1,170) and China the fourth most (351).[148]

The Recommendation appears to rely heavily on the type of reporting criticized by Brendan Kuerbis of the Internet Governance Project:

> [R]esearch and press stories driven by geopolitical conflict and national security concerns that equate transnational operators with governments (ala China Telecom) and treat them as adversaries are doing the global Internet a disservice. Getting details correct and substantiating claims with evidence matters.[149]

The Recommendation also notes that CTA is not currently a member of MANRS and erroneously accuses CTA of "disavow[ing] any responsibility to prevent routing errors."[150] To the contrary, CTA and its parent company have both devoted substantial resources for more than a year in an effort to incorporate the MANRS filtering standard into their global network, as required to become a member of MANRS.[151] This process is expensive and time-consuming because ChinaNet is the world's largest network in terms of customers served, and therefore has a huge number of routers and routes that have to be checked and upgraded. CTA and its affiliates have almost

---

[148] Robachevsky, Andrei, "14,000 Incidents: A 2017 Routing Security Year in Review", https://www.internetsociety.org/blog/2018/01/14000-incidents-2017-routing-security-year-review/.

[149] Kuerbis, *supra*.

[150] Recommendation, p. 48. Although some major U.S. network operators have joined MANRS as stated in the Recommendation, it is unclear whether these operators meet all of the MANRS standards with respect to all of the networks they operate. Further, some other major U.S. networks, including AT&T, Verizon, and Cox Communications, are not MANRS members. Non-membership is not a sufficient basis to infer poor network management practices.

[151] "Watch your MANRS: Akamai, Amazon, Netflix, Microsoft, Google, and pals join internet routing security effort", THE REGISTER, March 31, 2020, https://www.theregister.co.uk/2020/03/31/manrs_cdns/ ("China Telecom … reached out to us" and seems genuinely interested in working with MANRS to fix its issues, according to the Internet Society's senior director for technology programs, Andrei Robachevsky).

completed the preparatory work required by MANRS and plan on joining MANRS as soon as possible. If CTA and its parent were in fact focused on creating "opportunities" for the Chinese government to misroute U.S. communications traffic, they would have had no interest in implementing MANRS filtering.

E. CTA Responds Appropriately and Lawfully to Law Enforcement and National Security Requests.

As its final factor, the Recommendation asserts that the Executive Branch agencies "would not be able to work effectively with [CTA] to identify and disrupt unlawful activities or to assist in investigating unlawful conduct as the U.S. government currently does with trusted communications providers."[152] It claims that "[CTA's] indirect ownership and control by the Chinese government may result in particular sensitivities that could impair [its] compliance with lawful U.S. process that seeks *information transmitted* using networks connected to China."[153]

CTA's conduct to date does not demonstrate any reasonable basis for the U.S. government's stated lack of trust. CTA has been served with subpoenas or other legal process seeking information *about* its customers (as distinct from information transmitted by them), such as names, telephone numbers, account numbers, and the like, and it has provided this information in compliance with legal process, without exception. Over nearly 20 years of operation in the United States, CTA has never demonstrated any unwillingness to fulfill its legal obligations to provide information in response to lawful process.

The Recommendation also asserts that, in some cases, "U.S. authorities ***may*** have particular sensitivities that could limit sharing of information with [CTA] due to concerns that its …

[152] Recommendation, pp. 51-52.

[153] Recommendation, p. 52 (emphasis supplied).

Chinese affiliates would become aware of U.S. authorities' investigative interests in information related to [CTA's] services."[154] CTA's management is well aware of its legal obligations to comply with law enforcement and national security inquiries pursuant to lawful process, including, where applicable, obligations to keep information about such inquiries confidential. Again, in nearly 20 years of operations, CTA has never violated those obligations, and there is no basis for the U.S. government to speculate that it might do so in the future.

Finally, the Recommendation claims that CTA "has proven to be an untrustworthy and unwilling partner in the Executive Branch's mitigation efforts under the existing LOA," and therefore the agencies lack confidence in the effectiveness of any further mitigation.[155] This characterization is inaccurate.

CTA has communicated regularly and cooperatively with Team Telecom since at least 2007. On at least two occasions, Team Telecom staff have visited the CTA main office in Herndon, Virginia. CTA has notified Team Telecom of certain events for which notice was required under the LOA on approximately five occasions. Team Telecom also has occasionally requested CTA to confirm its compliance with the LOA, which CTA has done. Since CTA's current counsel began representing it in 2016, CTA has responded in writing to two questionnaires from Team Telecom in 2018 and 2019, as well as several follow-up questions posted in writing by Team Telecom. CTA's current counsel has exchanged correspondence and participated in teleconferences or meetings with Team Telecom on at least **90 occasions** since 2016.

---

[154] *Id.* (emphasis added).

[155] Recommendation, p. 53.

The Recommendation further bases its rejection of additional mitigation on an allegation that CTA has twice breached the existing LOA.[156] As discussed below, both of these claims — that CTA failed to adopt sufficient cybersecurity practices, and that it failed to notify Team Telecom about certain FCC filings — are unfounded.

1. CTA Complied with Its Information Security Obligations Under the LOA.

The Recommendation asserts that CTA "failed to take 'all practicable measures' to prevent unauthorized access to U.S. records" because CTA "did not implement a formal, comprehensive cybersecurity policy until December 2018."[157] The Recommendation also claims that CTA "did not create a privacy policy until 2016 and apparently did not post this policy on its website until after July 2017[.]"[158] These allegations misinterpret CTA's obligations under the LOA and misconstrue the facts as they relate to CTA's security policies and practices.[159]

a. CTA's Information Security Commitments to Team Telecom

CTA's commitments to Team Telecom regarding information security are reflected in the text of the CTA LOA. CTA agreed "to take all practicable measures to prevent unauthorized access to, or disclosure of the content of communications or U.S. Records, in violation of any U.S. Federal, state, or local law or of the commitments set forth in this letter."[160] The CTA LOA does not

[156] Recommendation, pp. 53-55.

[157] Recommendation, p. 54.

[158] Recommendation, p. 54.

[159] The Executive Branch agencies acknowledged in 2019 that CTA followed a range of security policies and procedures prior to December 2018. *See* Recommendation Exhibit 119 at EB-2745-46.

[160] Recommendation Exhibit 1 at EB-2.

require CTA to implement a single, comprehensive cybersecurity policy, or to post a privacy policy on its website. In fact, it does not require CTA to have any "written" information security document(s) or policy(ies) at all. Nor does CTA's LOA specify the provisions or issues that should be included, impose cybersecurity standards CTA must follow, or set a timeline for when such any specific policy or standard must be implemented.[161] Rather, the LOA left it to CTA to implement "practicable" measures appropriate to its network and services. Because the LOA is silent on specific requirements regarding CTA's information security policies, the fact that CTA fulfilled its obligations in a different manner than Team Telecom might have preferred cannot constitute a breach of the LOA. The Executive Branch agencies are trying to hold CTA to a standard that is simply not part of its LOA.

b. CTA's Information Security Policy Version 1.0 Memorialized Many Existing Policies.

CTA met its commitment in the LOA by consistently and continuously implementing and updating a variety of measures to prevent unauthorized access to or disclosure of U.S. Records that CTA actually collects and maintains in the course of provisioning and billing services to customers. Although the Information Security Policy provided in December 2018 was the "first formal, comprehensive security policy,"[162] it was not CTA's first (or only) policy governing its security practices.

---

[161] Team Telecom seems to have expected CTA to comply with obligations that are *not* in its LOA (and that Team Telecom never asked CTA to adopt), but that are in some more recent LOAs with other carriers. **[BEGIN CONFIDENTIAL]** [redacted] **. [END CONFIDENTIAL]**

[162] Recommendation Exhibit 37 at EB-655.

As CTA previously explained to Team Telecom, prior to December 2018, CTA maintained a variety of measures to prevent unauthorized access to its customer's records.[163] Specifically, CTA explained that **[BEGIN CONFIDENTIAL]** [redacted][164] **[END CONFIDENTIAL]** Before completing Version 1.0 in December 2018, CTA followed a number of its own written policies concerning information security, including **[BEGIN CONFIDENTIAL]** [redacted]. **[END CONFIDENTIAL]**[165]

CTA also has Physical Access Guidelines and Policies ("Physical Access Policies") that outline strict controls for access to CTA's POPs and data centers. Among other things, CTA's Physical Access Policies **[BEGIN CONFIDENTIAL]** [redacted].[166] [redacted]

[163] Recommendation Exhibit 103 at EB-2113.

[164] Recommendation Exhibit 36 at EB-590.

[165] Recommendation Exhibit 103 at EB-2113.

[166] CTA is a tenant, not an owner, of the buildings in which its POPs are located. These typically are "carrier hotel" buildings, and the owners and managers of these buildings enforce their own access controls in addition to those mandated by CTA for its facilities.

[redacted]. **[END CONFIDENTIAL]**

Moreover, CTA has always followed the standard industry practice of adhering to the securities set forth in the "house rules" established by the owners of facilities where CTA's Points of Presence are located and the data centers where data services are provided.[167] CTA's Physical Access Policies likewise require all visitors to CTA's POPs to adhere to the guidelines and policies of the relevant collocation or data center provider.

During the 11 years between execution of the LOA in 2007 and Team Telecom's June 2018 request for "copies of China Telecom Americas' cybersecurity policies and procedures,"[168] Team Telecom never inquired whether the company had one or more "written" cybersecurity policies or requested copies thereof. During these 11 years, CTA had multiple, lengthy check-in meetings with Team Telecom staff, but Team Telecom never, during those meetings or in any communications between meetings, provided any guidance on specific security measures that would be "mandatory" under the LOA.[169] And, Team Telecom's use of the plural forms in requesting "copies of China Telecom Americas' cybersecurity policies and procedures" inherently demonstrates that it would not be unreasonable for CTA to have more than one policy relevant to

[167] Recommendation Exhibit 103 at EB-2113.

[168] Recommendation Exhibit 32 at EB-576.

[169] *See* Recommendation Exhibit 124 at EB-2777-78.

cybersecurity.[170] The fact that several pre-existing security policies and procedures were not consolidated into a single, written document until December 2018 does not mean that the policies did not exist, that CTA failed to take measures to protect its customer information, or that it breached its obligations under the LOA.

2. The LOA Cannot Reasonably Be Construed to Require CTA to Have Notified Team Telecom of its ISPC Assignments.

The Recommendation also claims that CTA breached its LOA obligations because it "failed to inform the FBI, DOJ and DHS at least twice in 2010 when it filed notices to the FCC."[171] The "notices" in question were two requests for assignment of additional International Signaling Point Codes ("ISPCs") for use in connection with CTA's wholesale voice service[172] – a service that it has since stopped offering.[173] These requests were submitted using the "application" interface of the International Bureau Filing System ("IBFS"). This "application," however, is purely ministerial. The application form only requires the identity of the carrier and certification that the carrier understands and accepts the terms on which the code is assigned. The Commission performs no substantive review of this information. "After receipt of the ISPC application, the Commission

[170] This expectation also is consistent with more recent LOAs which require carriers to maintain Network Systems Security Plans, NIST-Compliant Cybersecurity Plans, and Information Security Plans which may be "combined into one or more documents[.]" **[BEGIN CONFIDENTIAL]** [redacted] **. [END CONFIDENTIAL]**

[171] Recommendation, p. 55.

[172] International Bureau File Nos. SPC-NEW-20100326-00007 and SPC-NEW-20100314-00006.

[173] *See* Exhibit 9.

assigns the ISPC code to each applicant (international carrier) free of charge on a first-come, first-served basis."[174]

Although the LOA requires CTA to notify Team Telecom "if there are any material changes in any of the facts represented in this letter or if it undertakes any action that require application to or notice to the FCC,"[175] this provision must be interpreted in its entirety and not by taking portions out of context. If the LOA only required CTA to advise Team Telecom of "material" changes in facts, it is reasonable to construe the requirement to advise of an "application" or "notice" to be limited to material FCC filings. The request for assignment of additional ISPCs was not a material change in CTA's business or services. In fact, CTA first obtained an ISPC in 2003, long before it signed the LOA (a fact known to the FCC and Team Telecom when CTA entered into the LOA).[176]

An interpretation of the LOA that requires prior notification to Team Telecom for trivial, ministerial filings with the FCC such as the ISPC assignment "application" would be unreasonable and inconsistent with the intent of the agreement. Nonetheless, even if the Commission did interpret the LOA to require such notification as the Recommendation urges, this "breach" would be immaterial and insubstantial, and would not rise to the level of justifying revocation of section 214 authorizations or, for that matter, even a lesser sanction of some sort. ISPCs are numbering resources, like area codes or NPA-NXX blocks, which carriers routinely request when their network operations require them. The Recommendation does not allege that the assignment of ISPCs without Team Telecom's knowledge caused any harm to the public interest. Under the circumstances,

---

[174] Information Collection Being Reviewed by the Federal Communications Commission Under Delegated Authority, 84 FR 56190 (Oct. 21, 2019).

[175] Recommendation Exhibit 1 at EB-2-3.

[176] International Bureau File No. SPC-NEW-20030314-00014.

it is hard to see how assignment of two new codes to a carrier that already held one could conceivably cause any such harm.

3. Team Telecom's Anticipatory Rejection of Additional Mitigation Measures is Unreasonable.

Finally, the Recommendation ventures into "through the looking glass" logic when it complains that CTA did not "propose additional mitigation when confronted with these breaches" (and, to boot, presupposes that any further mitigation that CTA might propose "would likely be insufficient").[177] As the Commission undoubtedly knows, companies do not propose mitigation measures to Team Telecom. Team Telecom dictates mitigation measures to companies, essentially on a take-it-or-leave-it basis. Without being asked, CTA is unable to guess what potential new mitigation measures Team Telecom might consider adequate. Also, without giving CTA the notice and opportunity to consider and carry out such new mitigation measures, it is unfair to jump to the conclusion that there will not be sufficient mitigation measures.

Indeed, the Administrative Procedure Act seems to require that the Commission give CTA an opportunity to mitigate any risks that it might identify. Assuming *arguendo* that there were grounds for the Commission to consider revocation of CTA's authorization — although there are not, as explained in Section II above — it would first have to give CTA an "opportunity to demonstrate or achieve compliance with all lawful requirements."[178] However, CTA cannot achieve compliance with all lawful requirements unless it is given notice of what steps are needed to do that.

The Commission directed CTA to respond to the allegations made by Team Telecom against it, and CTA has done so in this filing. Consistent with its conduct throughout its existence,

---

[177] Recommendation, p. 55.

[178] 5 USC § 558(c)(2).

CTA is focused on being an outstanding corporate citizen and was and is more than willing to address any issues raised by Team Telecom in order to mitigate any if their concerns and CTA regrets that it was not given this chance by Team Telecom before the Recommendation was filed.